Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

2
K&R

24. Jahrgang **Februar 2021** Seiten 73 – 144

dfv Mediengruppe · Frankfurt am Main

agenten). Daneben spielen vor allem Personal Information Management-Systeme (kurz „PIMS“) eine Rolle, bei denen die Dienstleistung im Vordergrund stehen. Diese zwischengeschalteten Systeme ermöglichen in der Regel die lokale Speicherung sowie die individuelle Verwaltung der eigenen personenbezogenen Daten, indem die betroffene Person auswählen kann, mit wem und wann sie welche Daten teilen möchte. Dadurch soll Dritten für konkrete Zwecke und bestimmte Zeiträume vorbehaltlich der von den natürlichen Personen selbst festgelegten Bedingungen und aller vom anzuwendenden Datenschutzrecht vorgesehenen Garantien die Verwendung personenbezogener Daten erlaubt werden.[33] Einige PIMS bieten die Möglichkeit, Daten über die Online-Präsenz des Nutzers (wie Browserverlauf, Lesezeichen, Adressbücher, Anmeldedaten, Ortungsdaten, Finanzdaten, Aktivitäten in sozialen Netzwerken) aufzuspüren und sie im PIMS zu organisieren.[34]

Einige dieser Anwendungen reichen bis zur vollständigen Fremdverwaltung der Daten der Nutzer (sog. Treuhand-Modelle), wie sie etwa im Bereich der Mobilitätsdaten[35] diskutiert werden. Treuhand-Modellen liegt der Gedanke zugrunde, dass diese Systeme kein über die Verwaltung hinausgehendes Eigeninteresse an den Daten haben und damit neutral und professionell agieren können.

Ziel aller sog. „Selbstschutz-Systeme“ ist die Befähigung des Einzelnen, seine personenbezogenen Daten zu kontrollieren und die Entlastung von Entscheidungen, die ihn überfordern.[36] Derzeit steckt diese Entwicklung allerdings noch in den Kinderschuhen.

VII. Fazit

Die Komplexität technisierter Verarbeitungsvorgänge führt bei alleinigem Abstellen auf eine Einwilligung zu einer unsachgemäßen Verlagerung von Abwägungs-Entscheidung auf den Betroffenen und zu Überforderungen. Die DSGVO bietet wegen der deklarierten Technikneutralität nur augenscheinlich zu wenige Antworten. Unter gebotener risikoorientierter Betrachtung sind bei genauerer Betrachtung auch hochkomplexe Datenverarbeitungen unter Einsatz innovativer Technologien möglich. Verantwortliche sollten sich dabei nicht vorschnell unter Rückgriff auf die Einwilligung ihrer Verpflichtungen aus Art. 5 DSGVO entledigt sehen. Das schon deshalb, weil sie gut beraten sind, vorab zu prüfen, ob ein ergänzender Rückgriff auf solche Rechtsgrundlagen, die einen angemessenen Ausgleich der betroffenen Grundrechtspositionen erlauben (vor allem Vertrag und berechtigte Interessen), möglich ist. Durch ein hohes Maß an Transparenz, Verteilung der Entscheidungshoheit zwischen Betroffenen und Verantwortlichen, unter Zuhilfenahme technischer Lösungen zur Stärkung der Datensouveränität sowie risikominimierende Technikgestaltung lassen sich so Fehleranfälligkeit und Widerruflichkeit der Einwilligung abfedern. Zugleich bieten Techniklösungen den Betroffenen heute neue Möglichkeiten, den Selbstdatenschutz zu stärken.

Zu wünschen ist auch, dass die Aufsichtsbehörden ihre Skepsis berechtigten Interessen und dem Gedanken der Kumulation von Rechtsgrundlagen gegenüber ebenso überdenken, wie eine allzu strenge Interpretation des Kopplungsverbotes.

Geht all dies Hand in Hand, wird Europa als Technologiestandort insgesamt gestärkt.

33 EDSB Stellungnahme 9/2016, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf, Rn. 53.
34 EDSB Stellungnahme 9/2016 (Fn. 33), Rn. 16.
35 *Brockmeyer*, ZD 2018, 258, 259.
36 DEK, Abschlussgutachten, S. 133 (Handlungsempfehlung Nr. 46) sowie S. 99 f., abrufbar unter https://datenethikkommission.de/wp-content/uploads/191028_DEK_Gutachten_bf.pdf.

RA Dipl.-Jur. Oliver Huq und RA Dr. Jan Verheyen*

Messenger datenschutzkonform in Unternehmen einsetzen

Kurz und Knapp

Die Kommunikation über „Sofortnachrichten“ („Instant-Messages“) verbreitet sich seit dem Einzug der Smartphones vor allem über mobile Apps (Stichwort „Mobile Messaging“) immer weiter. Auch für Unternehmen wird diese Art der Kommunikation für den Kunden- und Mitarbeiterkontakt immer interessanter. Auf Grund der Corona-Pandemie und der damit verbundenen vermehrten Auslagerung der Arbeit ins Homeoffice[1] hat sich dieser Trend noch zusätzlich beschleunigt. Der vorliegende Beitrag widmet sich dem Thema aus datenschutzrechtlicher Sicht und bewertet die aktuellen Möglichkeiten zur datenschutzkonformen Nutzung von Messengern in Unternehmen.

I. Messenger in Unternehmen

In Unternehmen stellt sich insbesondere seit der Einführung der DSGVO zum 25. 5. 2018 die Frage, inwieweit der Einsatz sogenannter Messenger-Dienste wie Facebook Messenger, iMessage, Signal, Telegram, Threema, WhatsApp und Co. rechtskonform möglich ist.[2] Viele Unternehmen erlauben ihren Mitarbeitern dabei die private Nutzung ihrer Firmen-Smartphones. Dadurch hat sich allein die Anzahl derjenigen, die ihr Smartphone außerhalb der Arbeitszeit für berufliches verwenden, im Zeitraum von 2017

* Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 30. 12. 2020.
1 Zum Datenschutz im Homeoffice vgl. *Verheyen/Elgert*, K&R 2020, 476.
2 Bezüglich WhatsApp s. *Hessel/Leffer*, CR 2020, 139.

bis 2019 verdoppelt.[3] Zu den Gefahren der dienstlichen Nutzung von Smartphones und Tablets sowie der Verwendung mitarbeitereigener Geräte gehören vor allem Verstöße gegen Sicherheits- und Datenschutzanforderungen – nicht zuletzt auch durch vom Benutzer privat installierter (Messaging-) Apps.[4] Vor allem der nach eigenen Angaben mit weltweit in über 180 Ländern vertretene und über 2 Milliarden Nutzer zählende Messenger WhatsApp ist derzeit auch in Deutschland der mit Abstand meistgenutzte Kommunikationsdienst.[5]

II. Messenger und Datenschutz

Unternehmen sind grundsätzlich gem. Art. 4 Nr. 7 DSGVO für die Erhebung und Verarbeitung personenbezogener Daten verantwortlich.[6] Dieser Grundsatz gilt auch beim Einsatz eines Messenger-Dienstes.[7] Die Verarbeitung personenbezogener Daten ist nach der DSGVO nur dann zulässig, sofern einer der in Art. 6 oder 9 DSGVO genannten Erlaubnistatbestände gegeben ist und die von der Verarbeitung betroffene Person zum Zeitpunkt der Datenerhebung gem. Art. 13 DSGVO informiert wird.

Die erste Frage, die sich stellt, ist die, ob und welche personenbezogenen Daten in und über den Messenger verarbeitet werden. In der Regel kommen hier die folgenden Daten in Frage:

- Kommunikationsdaten (Nutzername, Handynummer),
- Inhaltsdaten (Nachrichten zwischen Unternehmen und Nutzer, Medieninhalte),
- Meta-Daten des jeweiligen Messenger-Dienstes (dienen für gewöhnlich zur Verbindungsherstellung zwischen den Nutzern).

Wenn demnach personenbezogene Daten verarbeitet werden, sind die Vorschriften des Datenschutzes und hier insbesondere der DSGVO einschlägig und zu beachten. Da wie z. B. bei WhatsApp regelmäßig Telefonnummern und damit personenbezogene Daten[8] als Basis der Messenger-Kommunikation verwendet werden,[9] ist die DSGVO bei der Messenger-Nutzung im Unternehmen regelmäßig einschlägig.[10] Die sogenannte Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO gilt nur für rein private Nutzungen und scheidet für Unternehmen aus.

III. Zulässigkeit der Verarbeitung

Damit eine Verarbeitung personenbezogener Daten über einen Messenger zulässig ist, muss eine der folgenden Voraussetzungen erfüllt sein:

- Die betroffene Person hat in die Datenverarbeitung eingewilligt (Art. 6 Abs. 1 lit. a DSGVO).
- Die konkreten Daten dienen der Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO).
- Die konkrete Datenverarbeitung ist zur Wahrnehmung berechtigter Interessen erforderlich (Art. 6 Abs. 1 lit. f DSGVO).

Lediglich dann kann ein Unternehmen sicher sein, dass die Datenverarbeitung rechtskonform ist.

IV. In dubio pro Einwilligung

Oftmals ist der Einsatz eines Messengers nur über eine Einwilligung des jeweils betroffenen Personenkreises möglich und kann andernfalls sogar als deliktische Handlung aufgefasst werden.[11] Das gilt insbesondere bei der Kommunikation im Rahmen des Unternehmensmarketings, in der schon das Wettbewerbsrecht entsprechende Vorgaben macht (vgl. § 7 Abs. 3 UWG).

Voraussetzungen einer rechtskonformen Einwilligung sind:[12]

- Form: Eine Einwilligung kann formfrei (mündlich, elektronisch, Text- oder Schriftform) erteilt werden, es ist also keine gesonderte Form einzuhalten.
- Information: Der Einwilligende muss vorher klar und verständlich über Zweck und Umfang der die Einwilligung umfassenden Datenverarbeitung sowie über seine Rechte auf Löschung, Auskunft und Widerspruch informiert werden.
- Freiwilligkeit: Der Einwilligende muss eine echte Wahlfreiheit haben und die Einwilligung ohne zu erleidende Nachteile verweigern dürfen; hierauf ist er ebenfalls hinzuweisen.
- Eindeutige Bestätigung: Die Einwilligung muss klar bekundet werden (z. B. durch Unterschrift, konkludentes Verhalten, Opt-in; ein bloßes Opt-out (Möglichkeit zum Widerspruch) ist hier nicht ausreichend.
- Widerrufsmöglichkeit: Der Einwilligende muss seine Einwilligung jederzeit widerrufen können; dies ist in der Einwilligungserklärung klar zum Ausdruck zu bringen. Auf die Widerrufsmöglichkeit kann nicht verzichtet werden.
- Begrenzung: Jeder Einwilligende kann nur über seine eigenen personenbezogenen Daten verfügen; sollen die Daten mehrerer Personen verarbeitet werden, sind gesonderte Einwilligungen einzuholen.

Ohne eine entsprechende Einwilligung und mangels eines anderen Legitimationsgrundes werden personenbezogene Daten in unzulässiger Weise verarbeitet und der Datenschutz verletzt.

---

3 Deloitte GmbH Wirtschaftsprüfungsgesellschaft (Deloitte) – Smartphone-Nutzung am Limit? Der deutsche Mobile Consumer im Profil, Februar 2020, abrufbar unter: https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/smartphone-nutzung-2020.html.

4 Bundesamt für Sicherheit in der Informationstechnik (BSI) – IT-Grundschutz-Kompendium – Februar 2020, SYS. 3.1: Tablet und Smartphone, 2, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6.

5 Bundesnetzagentur – Nutzung von OTT-Kommunikationsdiensten in Deutschland – Bericht 2020, 2. Nutzung von OTT-Kommunikationsdiensten, 12, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile.

6 *Klabunde*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 4 Rn. 36 f.; *Hartung*, in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 4 Rn. 9; zur alten Rechtslage s. *Schrey/Kielkowski/Gola*, MMR 2017, 736, 737.

7 Für eine Abgrenzung der Verantwortungsbereiche zwischen Unternehmen und dem Messenger-Dienst *Jung/Hansch*, ZD 2019, 143, 145; grundlegend zu der sich in diesem Zusammenhang ebenfalls stellenden Frage einer gemeinsamen Verantwortlichkeit *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 Rn. 12 ff.; *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 26 Rn. 4 ff.

8 Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) – FAQ-Antwort – Was sind personenbezogene Daten? abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/FAQ/PersonenbezogeneDaten.php.

9 LDI NRW – Leitplanken für die Auswahl von Messenger-Diensten während der Kontaktbeschränkungen aufgrund der Corona-Pandemie, Stand: 18. 5. 2020, 1, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Schule_-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie/LDI-NRW- - -Messenger-Dienste-18_05_2020.pdf.

10 *Hessel/Leffer*, CR 2020, 139, 141; LDI NRW – Leitplanken für die Auswahl von Messenger-Diensten während der Kontaktbeschränkungen aufgrund der Corona-Pandemie (Fn. 9).

11 AG Bad Hersfeld, 20. 3. 2017 – F 111/17 EASO, ZD 2017, 435, Rn. 41, 165 ff. – Deliktische Handlung.

12 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) – Einwilligung, abrufbar unter: https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/MeineRechte/Artikel/Einwilligung.html; Frenzel, in: Paal/Pauly, DSGVO BDGS, 2. Aufl. 2018, Art. 6 Rn. 10 f.

Verantwortliche sind somit datenschutzrechtlich dazu verpflichtet, schon bei der ersten Datenerhebung (z. B. Verarbeitung von Namen und Handynummer) über Art, Zweck und Umfang der konkreten Datenverarbeitung zu informieren. Es empfiehlt sich hier die Bereitstellung der nötigen Datenschutzinformationen nach Art. 13 DSGVO z. B. über eine Webseite oder ein digital übermitteltes Dokument, das diese Informationen enthält.[13]

Auch die jeweiligen Datenschutzinformationen des konkreten Messenger-Anbieters sollten bereitgestellt werden[14] und – sofern möglich – ein Auftragsverarbeitungsvertrag abgeschlossen werden.[15]

V. Weitergabe von Kontaktdaten

Bei der erstmaligen Installation eines Messengers erfolgt in der Regel ein Zugriff auf das Adressbuch des Smartphones und die enthaltenen Kontaktinformationen werden an den jeweiligen Anbieter (z. B. WhatsApp Inc., das zur Facebook Inc. gehört und seinen Sitz in den USA hat) übermittelt.[16]

Geschieht das ohne die Zustimmung der hinter den Kontaktdaten stehenden Personen, liegt ein Verstoß gegen den Datenschutz vor.

Der Landesbeauftragte für den Datenschutz Niedersachsen (LfD NS) führt daher zu Recht spezifisch zum Messenger WhatsApp aus:[17]

„Es ergeben sich im Wesentlichen vier datenschutzrechtliche Problemstellungen:

- Die Übermittlung der Kontakte aus dem Adressbuch des Nutzers an WhatsApp.
- Die Übermittlung von personenbezogenen Daten in die USA.
- Die Nutzung von personenbezogenen Daten durch WhatsApp.
- Die Übermittlung der Nutzerdaten an andere Unternehmen des Facebook-Konzerns“

„Eine datenschutzkonforme Nutzung von WhatsApp ohne Übertragung von Telefonnummern ist also nur bei dauerhafter Deaktivierung des Zugriffs auf die Kontakte direkt nach der Installation möglich.“

Der LfD NS stellt hierzu auch ein Merkblatt für die Nutzung von WhatsApp in Unternehmen zum Download bereit.[18] Die Ausführungen des LfD NS sind allerdings insofern veraltet, als dass sie das EuGH-Urteil zum Privacy Shield[19] noch nicht berücksichtigen.

Die nicht autorisierte Weitergabe von Kontaktdaten seitens eines Unternehmens an den jeweiligen Messenger-Anbieter muss aus datenschutzrechtlicher Sicht also in jedem Fall vermieden werden. Hierzu kommen verschiedene Maßnahmen in Frage:

- Installation einer App auf dem jeweiligen Endgerät, die den Messenger „bändigt“, oder eine sogenannte Containerlösung, die Datenbestände auf dem Endgerät „auseinanderhält“.[20]
- Es können auch schlicht Smartphones ohne Kontaktdaten verwendet werden, auf denen dann nach und nach nur Kontakte eingetragen werden, die der Verarbeitung ihrer Daten ordnungsgemäß zugestimmt haben.[21]
- Eine weitere Option ist der Einsatz spezialisierter Dienstleister, die über eine sogenannte Software-as-a-Service(SaaS)-Plattform die Nutzung aller gängigen Messenger über einen Dienst ermöglichen, ohne dass der jeweilige Messenger auf einem eigenen Endgerät installiert werden muss und ohne dass personenbezogene Daten an die Messenger-Anbieter übertragen werden.[22]

Um eine ungewollte und unzulässige Verarbeitung personenbezogener Daten zu verhindern, können also verschiedene (technische) Lösungen eingesetzt werden. Im Einzelnen sollte mit der eigenen IT und/oder einem externen Experten zur IT-Sicherheit abgeklärt werden, welche Lösung auf dem Stand der Technik den eigenen Anforderungen und dem jeweiligen Budget am ehesten entspricht.

Zur datenschutzkonformen Nutzung von Messenger-Diensten ist es in jedem Fall erforderlich, den ungewollten Datenzugriff auf die Kontaktdaten aus den gespeicherten Adressbüchern zu unterbinden; Entsprechendes gilt für alle anderen personenbezogenen Daten, die mit einem Messenger ebenfalls übertragen werden.

VI. Übermittlungen ins außereuropäische Ausland

Viele Messenger-Dienste, ebenso wie viele andere Datenverarbeitungsdienste, werden von Firmen außerhalb der EU angeboten und neben den USA sind insbesondere Australien, Chile, China, Indonesien, Israel, Japan, Kanada, Neuseeland, Saudi-Arabien, Süd-Korea, Thailand u. a. Staaten, in denen viele Technologiekonzerne angesiedelt sind.[23]

Gerade die USA sind mit Apple (FaceTime, iMessage), Facebook (Instagram, Messenger, WhatsApp), Google (Hangouts, Messages), Microsoft (Skype), Signal Technology Foundation (Signal) und Snap Inc. (Snapchat) überdurchschnittlich häufig vertreten bei den derzeit meistgenutzten Messenger-Diensten.[24] Daneben wird Telegram derzeit nach Angaben auf der Entwickler-Webseite aus Dubai heraus weiter aufgebaut,[25] die Threema GmbH (verantwortlich für Threema) ist ein Schweizer Unternehmen[26]

13 Für die Form und Darstellung s. auch *Mester*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 13 Rn. 36.

14 So z. B. von Threema, abrufbar unter: https://threema.ch/de/privacy; Telegram, abrufbar unter: https://telegram.org/privacy; Signal, abzurufen unter: https://signal.org/legal/#privacy-policy.

15 Z. B. möglich bei Beekeeper, abrufbar unter: https://docs.google.com/document/d/1UfUdqljDUsX3J-43_tvl2SCdGTzPFfYYUtx9srCwDv4/preview und Threema, abrufbar unter: https://work.threema.ch/docs/_threema_avv.pdf.

16 Für die Beschreibung des Vorgangs bei WhatsApp vgl. *Hessel/Leffer*, CR 2020, 139.

17 LfD NS – Nutzung von WhatsApp in Unternehmen, abrufbar unter: https://lfd.niedersachsen.de/startseite/themen/wirtschaft/nutzung-von-whatsapp-in-unternehmen-179649.html.

18 LfD NS – Merkblatt für die Nutzung von „WhatsApp“ in Unternehmen, abrufbar unter: https://lfd.niedersachsen.de/download/132861/Merkblatt_fuer_die_Nutzung_von_WhatsApp_in_Unternehmen.pdf.

19 EuGH, 16. 7. 2020 – C-311/18, K&R 2020, 588 – Schrems II.

20 Als App für Android käme z. B. XPrivacyLua in Frage, vgl.: https://lua.xprivacy.eu.

21 Diese einfache Lösung erfordert allerdings eine erhebliche Mitarbeiter-Disziplin und wird nach allgemeiner Lebenserfahrung im Betriebsalltag nur schwerlich von allen Mitarbeitern durchzuhalten sein.

22 Solche Lösungen werden u. a. z. B. angeboten von Casengo, abrufbar unter: https://www.casengo.com/de; Messengerpeople, abrufbar unter: https://www.messengerpeople.com/; Trengo, abrufbar unter: https://trengo.com/en; Userlike, abzurufen unter: https://www.userlike.com/de/; Zendesk, abrufbar unter: https://www.zendesk.de/.

23 Vgl. Contor Unternehmensberatung – Studie Technologiestandorte Weltweit, abrufbar unter: https://www.thema-standortanalyse.de/e-books-zur-standortanalyse/technologiestandorte-welt/.

24 Bundesnetzagentur – Nutzung von OTT-Kommunikationsdiensten in Deutschland – Bericht 2020, 2. Nutzung von OTT-Kommunikationsdiensten, 12, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile.

25 Telegram, Fragen und Antworten, abzurufen unter: https://telegram.org/faq#f-wo-ist-der-standort-von-telegram.

26 Threema GmbH, Über uns, abrufbar unter: https://threema.ch/de/about.

und Viber wird von der japanischen Firma Rakuten K. K. entwickelt.[27]

In der Europäischen Union schützen nationale Gesetze und europäische Verträge die Grundrechte der Bürger auf Datenschutz.[28] Um US-amerikanischen Unternehmen die Verarbeitung von (europäischen) personenbezogenen Daten in den USA zu ermöglichen, wurden die sogenannten Regeln des sicheren Hafens („Safe Harbor"[29]) und dann der sogenannte „EU-US Privacy Shield"[30] vereinbart. Sowohl „Safe Harbour" als auch „Privacy Shield" dienten der Herstellung eines angemessenen Schutzniveaus personenbezogener Daten von EU-Bürgern auch in den USA und waren jeweils durch eine Entscheidung[31] bzw. einen Angemessenheitsbeschluss[32] der EU-Kommission bis zur jeweiligen Aufhebung durch den EuGH anerkannt.

Somit gilt derzeit und solange keine den Datenschutz nach der DSGVO auch in den USA gewährende Vereinbarung getroffen wird, dass die Übermittlung von personenbezogenen Daten in die USA momentan nur dann rechtlich zulässig ist, wenn sogenannte EU-Standardvertragsklauseln[33] oder Binding Corporate Rules[34] greifen. Im Umkehrschluss ist also die bisher nur auf den „EU-US Privacy-Shield" gestützte Datenverarbeitung personenbezogener Daten in den USA rechtswidrig.

Darüber hinaus hat die EU-Kommission entschieden, dass ein angemessenes Datenschutzniveau in Andorra, Argentinien, auf den Färöer-Inseln, Guernsey, Israel, der Isle of Man, Japan, Jersey, Kanada, Neuseeland, der Schweiz und Uruguay gilt. Das bedeutet, dass in diese Länder ebenfalls datenschutzkonform personenbezogene Daten übermittelt und dort verarbeitet werden dürfen.[35] Gleiches gilt für die drei außerhalb der EU liegenden, aber zum Europäischen Wirtschaftsraum (EWR) gehörenden Staaten Island, Liechtenstein und Norwegen.[36]

Folglich sollten, falls noch nicht geschehen, Unternehmen nach der Schrems II-Entscheidung des EuGH schnellstmöglich auf DSGVO-konforme Messenger-Alternativen umsteigen.

VII. Verzeichnis über Verarbeitungstätigkeiten

Schließlich sollte immer auch an die ordnungsgemäße Dokumentation aller für den Datenschutz relevanten Verarbeitungsvorgänge im sogenannten Verzeichnis über Verarbeitungstätigkeiten nach Art. 30 DSGVO (auch Verarbeitungsverzeichnis genannt[37]) gedacht werden. Das Verzeichnis ist schriftlich zu führen[38] und dient dem Nachweis der Einhaltung der DSGVO.[39] Es ist zudem auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.[40]

Für die Messenger-Kommunikation sollte darüber hinaus zur besseren Übersicht im bestehenden Verarbeitungsverzeichnis ein eigener Bereich (ggfs. unterteilt in Unterkategorien wie z. B. Marketing, Mitarbeiterkommunikation, Kundenkommunikation (Service) etc.) mit der üblichen und rechtskonformen Dokumentation vorgesehen werden.

VIII. Besondere Kategorien personenbezogener Daten

Dass selbst in Bereichen, in denen hochsensible, persönliche Daten (sogenannte besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO) verarbeitet werden, der Einsatz von Messengern möglich ist, belegt das „Whitepaper" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).[41] In diesem werden „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich" formuliert.

Die dort erläuterten technischen Anforderungen gelten zur Verwendung im Krankenhaus, können darüber hinaus aber auch als Blaupause für andere Bereiche dienen, in denen erhöhte Anforderungen an den Datenschutz bei der Verwendung von Messengern gestellt werden. Gerade Unternehmen, die personenbezogene Daten nach Art. 9 DSGVO verarbeiten, sollten die im „Whitepaper" geschilderten Anforderungen daher kennen und – soweit möglich – umsetzen.

IX. Fazit

Die Verwendung von Messengern in Unternehmen ist selbst in Bereichen möglich, in denen erhöhte Datenschutzanforderungen gefragt sind (Gesundheitswesen, Personalwesen etc.). Doch eine Nutzung vieler Messenger wie z. B. WhatsApp ist nicht ohne Weiteres datenschutzkonform möglich. Vielmehr ist eine gründliche Planung und Bedarfsanalyse in Abstimmung mit dem Datenschutzbeauftragten (und/oder Datenschutzexperten) und der IT und/oder externen IT-Sicherheitsexperten unumgänglich.

Von der Nutzung von WhatsApp als am weitesten verbreitetem Messenger ist – sofern die einschlägigen Datenschutzbestimmungen beachtet werden sollen – zurzeit und sofern nicht konkrete und wirksame Maßnahmen zur datenschutzkonformen Nutzung ergriffen werden – abzuraten.

Es gibt jedoch Alternativen wie beispielsweise Threema[42] sowie technische Möglichkeiten um die Messenger-Nutzung DSGVO-konform zu gestalten.

---

27 Rakuten – About Us, abrufbar unter: https://global.rakuten.com/corp/about/de/.

28 Art. 8 Charta der Grundrechte der EU; Art. 16 Vertrag über die Arbeitsweise der EU; und die auf den vorstehenden beiden Bestimmungen erlassene DSGVO.

29 Wurde vom EuGH für unwirksam erklärt: EuGH, 6. 10. 2015 – C-362/14, K&R 2015, 710 ff., abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62014CJ0362&from=DE – Safe-Harbor.

30 Wurde ebenfalls vom EuGH für unwirksam erklärt: EuGH, 16. 7. 2020 – C-311/18, K&R 2020, 588 – Schrems II.

31 Entscheidung der Kommission, 26. 7. 2000 – K(2000) 2441, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=uriserv:OJ.L_.2000215. 1. 0007.01.DEU – sicherer Hafen.

32 Durchführungsbeschluss (EU) 2016/1250 der Kommission, 12. 7. 2016 – C(2016) 4176, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016D1250&from=DE – „EU-US-Datenschutzschild".

33 So beispielsweise der Hessische Beauftragte für Datenschutz und Informationsfreiheit, abrufbar unter: https://datenschutz.hessen.de/datenschutz/internationales/eu-standardvertragsklauseln.

34 Soweit nach Art. 47 DSGVO durch die zuständige Aufsichtsbehörde genehmigt. In der DSGVO ist insoweit von verbindlichen internen Datenschutzvorschriften die Rede.

35 Liste der aktuell bestehenden Angemessenheitsbeschlüsse der EU Kommission – Adequacy decisions, abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

36 Im europäischen Wirtschaftsraum (EWR) gilt die DSGVO seit dem 6. 7. 2018 unmittelbar: Beschluss des Gemeinsamen EWR-Ausschusses, 6. 7. 2018 – Nr. 154/2018, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:22018D1022&from=DE.

37 Vgl. z. B. Bitkom e. V. – Das Verarbeitungsverzeichnis, abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-online.pdf.

38 Wobei hier die elektronische Form ausreichend ist, Art. 30 Abs. 3 DSGVO.

39 DSGVO Erwägungsgrund 82.

40 Art. 30 Abs. 4 DSGVO.

41 DSK, 7. 11. 2019 – Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf.

42 Für einen guten Überblick s. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055.