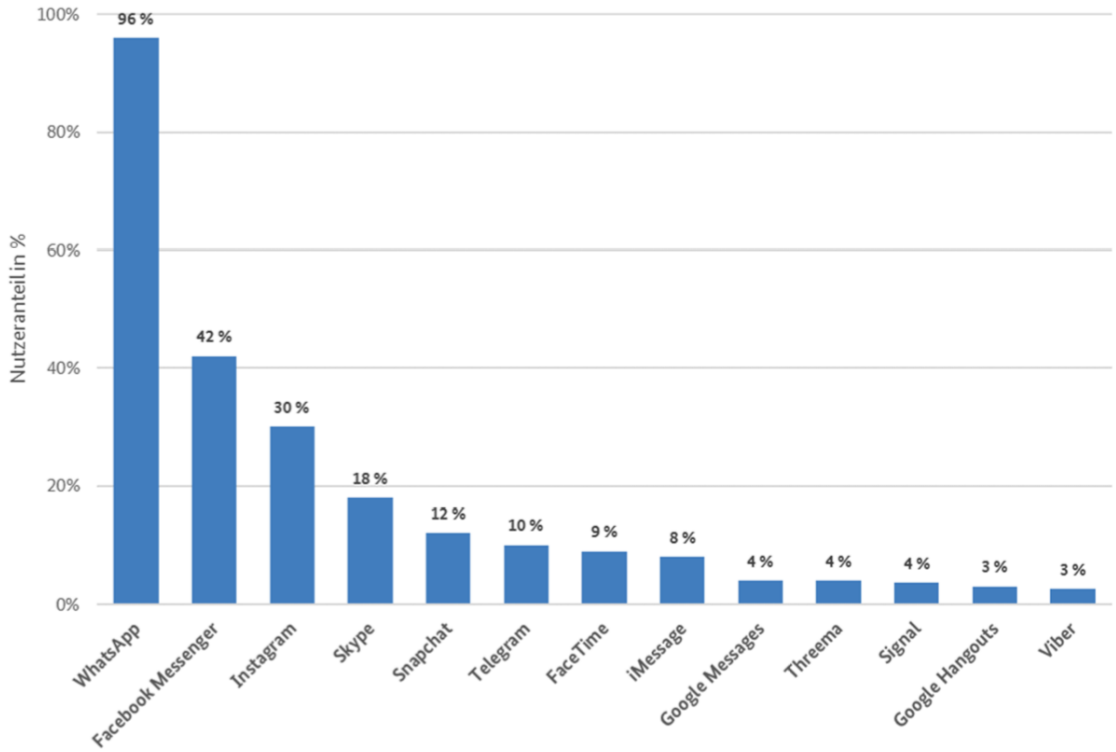
Messenger datenschutzkonform in Unternehmen einsetzen

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.

In Unternehmen stellt sich insbesondere seit der Einführung der DSGVO zum 25. Mai 2018 die Frage, inwieweit der Einsatz sogenannter Messenger-Dienste wie Facebook Messenger, iMessage, Signal, Telegram, Threema, WhatsApp und Co rechtskonform möglich ist. Viele Unternehmen erlauben Ihren Mitarbeitern die private Nutzung Ihrer Firmen-Smartphones, ohne vorher jedoch die Möglichkeiten und Risiken zu beleuchten. Vor allem der nach eigenen Angaben mit weltweit in über 180 Ländern vertretene und über 2 Milliarden Nutzern zählende Messenger WhatsApp[i] ist auch in Deutschland der mit Abstand meistgenutzte Kommunikationsdienst derzeit.[ii]

Abbildung 4: Nutzungsanteile OTT-Kommunikationsdienste



Quelle: Eigene Darstellung. Basis: Nutzer OTT-Kommunikationsdienste (Mehrfachnennungen möglich), n = 1.858. Die nicht abgebildeten OTT-Kommunikationsdienste sind im Folgenden nach absteigenden Nutzeranteilen aufgeführt: Line (2 %), Google Duo (1 %), WeChat (1 %) und Sonstige (jeweils unter 0,5 %).

Quelle: Bundesnetzagentur[iii][iv]

Es folgen einige Empfehlungen für die Praxis zur datenschutzkonformen Kommunikation über Messenger-Dienste im Unternehmen.

1. Beachtung des Datenschutzes

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

Die erste Frage, die sich stellt, ist insoweit, 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, etc.)
- Inhaltsdaten (Nachrichten zwischen Unternehmen und Nutzer, Medieninhalte etc.)
- Meta-Daten des jeweiligen Messenger-Dienstes (dienen i.d.R. zur Verbindungsherstellung zwischen den Nutzern)

Wenn also personenbezogene Daten verarbeitet werden, dann sind auch die Vorschriften des Datenschutzes und hier insbesondere der DSGVO einschlägig und zu beachten.

HINWEIS: Wenn zudem vertrauliche Unternehmensinformationen (Geschäftsgeheimnisse etc.) übermittelt werden (sollen), dann können neben den Vorschriften des Datenschutzes auch andere Vorschriften und Gesetze wie z.B. das Gesetz zum Schutz von Geschäftsgeheimnissen einschlägig sein.

2. Zulässigkeit der Verarbeitung

Ein der folgenden Voraussetzungen muss erfüllt sein, damit eine Verarbeitung personenbezogener Daten[vi] über einen Messenger zulässig ist:

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

Es sollte also zunächst geprüft werden, ob mindestens eine der genannten Alternativen zutrifft. Ist zumindest eine Legitimationsgrundlage gegeben, dann darf die Datenverarbeitung erfolgen.

3. **In dubio pro „Einwilligung“**

Oftmals ist der Einsatz eines Messenger nur über eine Einwilligung des jeweils betroffenen Personenkreises möglich.[viii] Das gilt insbesondere bei der Kommunikation im Rahmen des Unternehmensmarketings.[ix]

Voraussetzungen einer rechtskonformen Einwilligung:

- 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[x]
- Freiwilligkeit[xi]: 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 den Widerruf kann nicht verzichtet werden!
- Begrenzung: Jeder Einwilligende kann nur über seine eigenen personenbezogenen Daten verfügen; sollen die Daten mehrerer Personen verarbeitet werden, dann sind entsprechend gesonderte Einwilligungen einzuholen

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

Verantwortliche sind 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).

Auch die jeweiligen Datenschutzinformationen des konkreten Messenger-Anbieters sollten bereitgestellt werden (so z.B. von Threema (https://threema.ch/de/privacy); Telegram (https://telegram.org/privacy); Signal (https://signal.org/legal/#privacy-policy)) und – sofern möglich – ein Auftragsverarbeitungsvertrag abgeschlossen werden (z.B. möglich bei Teamwire und Threema).

4. Vertrauen ist gut, Kontrolle ist besser

Bei der erstmaligen Installation eines Messengers erfolgt in der Regel ein Zugriff auf das Adressbuch des jeweiligen 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.

In der Regel geschieht das ohne die Zustimmung der hinter den Kontaktdaten stehenden Personen und es liegt in diesem Fall ein Datenschutzverstoß vor.

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

> *„Es ergeben sich im Wesentlichen vier datenschutzrechtliche Problemstellungen:*
>
> 1. *Die Übermittlung der Kontakte aus dem Adressbuch des Nutzers an WhatsApp.*
> 2. *Die Übermittlung von personenbezogenen Daten in die USA.*
> 3. *Die Nutzung von personenbezogenen Daten durch WhatsApp.*
> 4. *Die Übermittlung der Nutzerdaten an andere Unternehmen des Facebook-Konzerns"*[xii]

Weiter kommt er zu nach weitergehender Prüfung zu folgendem, ebenfalls korrektem Schluss:

> *„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.[xiii] Diese Ausführungen sind allerdings insofern veraltet, als dass Sie das EuGH-Urteil zum Privacy Shield noch nicht berücksichtigen.

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

- Installation einer App auf dem jeweiligen Endgerät, die den Messenger „bändigt" oder eine sogenannte Containerlösung, die Datenbestände auf dem Endgerät „auseinanderhält".[xiv]
- Es können auch einfach „nackte" Smartphones ohne Kontaktdaten verwendet werden auf denen dann nach und nach nur Kontakte eingetragen werden auf, die der Verarbeitung Ihrer Daten ordnungsgemäß zugestimmt haben.[xv]
- 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 das der jeweilige Messenger auf einem eigenen Endgerät installiert werden muss und ohne, dass personenbezogene Daten an die Messenger-Anbieter übertragen werden.[xvi]

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

Zur datenschutzkonformen Nutzung von Messenger-Diensten ist es in jedem Fall nötig, den ungewollten Datenzugriff auf die Kontaktdaten aus den gespeicherten Adressbüchern zu unterbinden.

5. Übermittlungen ins Ausland außerhalb der EU

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, Neu Seeland, Saudi Arabien, Süd Korea, Thailand u.a. Staaten, in denen viele Technologiekonzerne angesiedelt sind.[xvii]

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

In der Europäischen Union schützen nationale Gesetze und europäische Verträge die Grundrechte der Bürger auf Datenschutz. Um US-amerikanischen Unternehmen die Verarbeitung von personenbezogenen Daten in den USA zu ermöglichen, wurden zunächst die sogenannten Regeln des sicheren Hafens („Safe Harbor“ – wurde am 06.10.2015 für ungültig erklärt[xix]) und dann der sogenannte EU-US Privacy Shield (wurde am 16.07.2020 für ungültig erklärt) vereinbart. Sowohl Safe Harbour als auch der Privacy Shield sollten ein angemessenes Schutzniveau personenbezogener Daten von EU-Bürgern auch in den USA gewährleisten.

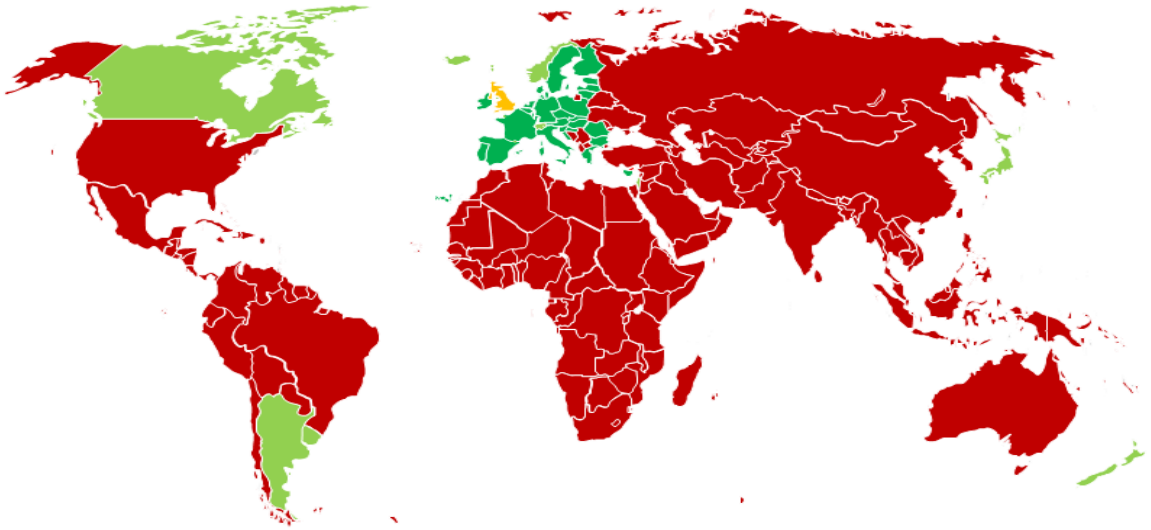
Somit gilt derzeit und solange keine den Datenschutz nach der DSGVO auch in den USA gewährende Vereinbarung getroffen wird, dass die Übermittlung von personenbezogenen Daten in die USA momentan nur dann rechtlich zulässig ist, wenn sogenannte EU-Standardvertragsklauseln[xx] oder Binding Corporate Rules[xxi] (in der DSGVO als verbindliche interne Datenschutzvorschriften bezeichnet[xxii]) 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 Faroer Inseln, Guernsey, Israel, der Isle of Man, Japan, Jersey, Kanada, Neu Seeland, die Schweiz und Uruguay gilt. Das

bedeutet, dass in diese Länder, über drei außerhalb der EU liegenden aber zum Europäischen Wirtschaftsraum (EWR) gehörenden Staaten Island, Liechtenstein und Norwegen – im EWR gilt die DSGVO seit dem 06.07.2020 unmittelbar – hinaus ebenfalls datenschutzkonform auch personenbezogene Daten übermittelt und dort verarbeitet werden dürfen.

Einen guten Überblick gewährt die folgende Darstellung:

DSGVO-Atlas - Angemessenes Datenschutzniveau



- DSGVO konformer Datenschutz nicht gewährleistet
- EWR & EU-Kommission: Datenschutz gewährleistet
- EU-Mitgliedstaaten: Datenschutz gewährleistet
- UK: Brexit – Datenschutzniveau unklar Übergangsphase bis zum 31.12.2020

Weltweiter Datenschutz: Im größten Teil der Welt wird EU-Datenschutzniveau **nicht** gewährleistet

Darstellung: Oliver Huq, Stand 11/2020

Dementsprechend stellt sich seit dem Urteil des EuGH im Sommer verstärkt die Frage nach (DSGVO-konformen) Messenger-Alternativen zu WhatsApp und Co.

6. DSGVO-konforme WhatsApp-Alternativen

Ein kleiner Überblick[xxiii] über DSGVO-konforme, allgemeine mobile Messenger-Alternativen, die den Datenschutz beachten sowie spezieller Messenger für Unternehmen:

- **Beekeper**
  - Messenger speziell für Unternehmen
  - DSGVO-konform
  - Anbieter: Beekeeper AG, Zürich, Schweiz
  - Preis: auf Anfrage

- **ginlo**
  - Messenger für Privatpersonen und Unternehmen
  - DSGVO-konform
  - Anbieter: ginlo.net Gesellschaft für Datenkommunikationsdienste mbH, München, Deutschland
  - Preis: für Privatnutzer kostenfrei/für Unternehmen: ab 1,43 EUR/Monat und Nutzer[xxiv]

- **iMessage**[xxv]
  - Messenger für „alle iOS-Nutzer"
  - DSGVO-konform („Zero-Knowledge-Prinzip" und sofern entsprechende Voreinstellungen vorgenommen werden)
  - Anbieter: Apple Inc., Cupertino, Ca, USA
  - Preis: kostenlos

- **Signal**
  - Messenger für „alle"
  - DSGVO-konform („Zero-Knowledge-Prinzip")
  - Anbieter: Signal Foundation, Mountain View, CA, USA
  - Preis: kostenlos

- **Teamwire**
  - Messenger speziell für Unternehmen
  - DSGVO-konform
  - Anbieter: Teamwire GmbH, München, Deutschland
  - Preis: Device- und Nutzer-Lizenzen auf Anfrage

- **Telegram**
  - Messenger für Privatpersonen und Unternehmen
  - DSGVO-konformität mit entsprechenden Voreinstellungen möglich
  - Anbieter: Pavel und Nikolai Durov, Dubai, VAE
  - Preis: kostenlos

- **Threema**
  - Messenger für Privatpersonen und Unternehmen
  - DSGVO-konform
  - Anbieter: Threema GmbH, Pfäffikon, SZ, Schweiz
  - Preis: ab 3,99 EUR (einmalig); Threema Work, ab 1,40 CHF/Gerät und Monat und auf Anfrage

- **Wire**
  - Messenger für Privatpersonen und Unternehmen
  - DSGVO-konform
  - Anbieter: Wire Swiss GmbH, Zug, Schweiz
  - Preis: zur privaten Nutzung kostenlos; ab 5 EUR/Monat und Nutzer

7. Verzeichnis über Verarbeitungstätigkeiten

Last but not least 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) gedacht werden. Im Zweifel kann so die Einhaltung des Datenschutzes bei Bedarf schriftlich nachgewiesen werden.

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

8. Besondere Kategorien personenbezogener Daten

Dass selbst in Bereichen, in denen höchstsensible, 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 unabhängige Datenschutzaufsichtsbehörden des Bundes und der Länder vom 07.11.2019.[xxvii] In diesem werden „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich" formuliert.

Die in dem entsprechenden Dokument erläuterten technischen Anforderungen gelten zur Verwendung im Krankenhaus. Sie können darüber hinaus 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 kennen und möglichst umsetzen.

9. Fazit

Die Verwendung von Messengern in Unternehmen ist selbst in Bereichen möglich, in denen erhöhte Datenschutzanforderungen gefragt sind (Gesundheitswesen, Personalwesen etc.). Doch eine Nutzung von WhatsApp & Co ist nicht ohne weiteres datenschutzkonform. 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 kann – sofern die einschlägigen Datenschutzbestimmungen beachtet werden sollen – zur Zeit und sofern nicht konkrete und wirksame Maßnahmen zur datenschutzkonformen Nutzung ergriffen werden können – nur abgeraten werden.

Es stehen jedoch eine Vielzahl datenschutzkonformer und mindestens gleichwertiger Alternativen zur Verfügung.

10. Vertiefende Lese-Empfehlungen

Das Thema ist sehr komplex und neben den bereits in den Endnoten angegebenen Links möchte ich Ihnen noch einige informative und wie ich finde auch hilfreiche Leseempfehlungen mit an die Hand geben:

- Verbraucherzentrale: „WhatsApp-Alternativen: Messenger im Überblick“, Stand 13.10.2020
- Verbraucherzentrale: „Datenschutz bei Messengern im Überblick“ (Stand: 30.01.2020
- bitkom: „Wie Sie die DSGVO mit ECM-Lösungen praxisgerecht einhalten – Leitfaden“, Stand: 2018
- ULD: „Datenschutz: Plötzlich im Homeoffice – und nun?“, Stand: März 2020
- BfDI: „Telearbeit und Mobiles Arbeiten“, Stand: Juli 2020
- GDD: „Datenschutz und Corona – Videokonferenzen, Mobiles Arbeiten und HomeOffice – „Ausgewählte Beiträge zu den Themen Datenschutz und Datensicherheit“, Linksammlung, Stand: 30.10.2020
- bitkom: „Links zur Unterstützung aus dem Digital Office“
- Bundeskartellamt: Das Amt teilt am 12.11.2020 mit, dass es eine Sektor-Untersuchung zu Messenger-Diensten einleitet. Es führt hierzu aus:

  „In den kommenden Monaten wird das Bundeskartellamt die Branche und Experten zu diesen und anderen Themen mündlich und schriftlich befragen. Nach Abschluss der Ermittlungen werden die Ergebnisse in einem Bericht der Öffentlichkeit vorgestellt.
  Das Bundeskartellamt kann im Bereich Verbraucherschutz Untersuchungen durchführen und so etwaige Verstöße sowie mögliche Defizite in der Rechtsdurchsetzung identifizieren. Die Befugnis, aufgedeckte Rechtsverstöße auch per behördlicher Verfügung abzustellen, ist damit bislang hingegen nicht verbunden.“

  Weitere Informationen entnehmen Sie der Pressemitteilung des Amtes unter: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_SU_Messenger_Dienste.html

DER AUTOR

Dipl. Jur. Oliver Huq ist Rechtsanwalt bei Schumacher & Partner in Düsseldorf.

Er berät u.a. mit den Schwerpunkten IT-/IP- und Vertrags-Recht sowie im gewerblichen Rechtschutz, im Bereich Compliance (inkl. Kartell- und Wettbewerbsrecht) und Datenschutz.

https://schumacherundpartner.de/oliver-huq/

[i] https://www.whatsapp.com/about/, abgerufen am 05.11.2020
[ii] Mit 96 % vor dem Facebook Messenger (42 %), Instagram (30 %), Skype (18 %), Snapchat (12 %), Telegram (10 %), FaceTime (9%), iMessage (8 %), Google Messages (4%), Threema (4 %) Signal (4 %), Google Hangouts (3 %) und Viber (3 %) (vgl. https://www.messengerpeople.com/de/studie-messenger-nutzung-2020-deutschland/#:~:text=Welche%20sind%20die%20beliebtesten%20Messenger%20in%20Deutschland%3F&text=Innerhalb%20der%20Gruppe%20von%20OTT,12%20%25)%20am%20weitesten%20verbreitet (abgerufen am 05.11.2020)
[iii] https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile (abgerufen am 11.11.2020)
[iv] vgl._ https://www.messengerpeople.com/de/studie-messenger-nutzung-2020-deutschland/#:~:text=Welche%20sind%20die%20beliebtesten%20Messenger%20in%20Deutschland%3F&text=Innerhalb%20der%20Gruppe%20von%20OTT,12%20%25)%20am%20weitesten%20verbreitet (abgerufen am 05.11.2020)
[v] Vgl. Art. 6 und Art. 9 DSGVO
[vi] „Verarbeitung" [bezeichnet] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;" (vgl. Art. 4 Nr. 2 DSGVO)
[vii] Vgl. hierzu Erwägungsgund 47 und Erwägungsgrund 48 zur DSGVO
[viii] Nur wenn die Datenverarbeitung zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen notwendig ist oder wenn die Legitimation über berechtigte Interessen des Verarbeitenden erfolgt, wird keine Einwilligung benötigt. Nur in diesen Fällen ist die Verarbeitung datenschutzrechtlich auch ohne eine Einwilligung legitimiert (vgl. Art. 6 Abs.1 lit. B & lit. f DSGVO).
[ix] Auch Marketing- und Vertriebszwecke eines Unternehmens können als berechtigtes Interesse die Datenverarbeitung legitimieren; das gilt zumindest dann, wenn überwiegende Interessen und/oder Grundrechte des Betroffenen dem nicht entgegenstehen. Das wäre z.B. der Fall, wenn sich die Datenverarbeitung über den verwendeten Messenger im vernünftigerweise vom Nutzer bei der Kommunikation zu erwartenden und üblichen Rahmen bewegt. Das dürfte bei der Verwendung von Messengern etwaiger Drittanbieter (wie z.B. WhatsApp) z.B. aufgrund der Datenübertragung und -speicherung in den USA nicht der Fall sein. Beim Einsatz solcher Drittanbieter-Messenger sollte zur Legitimation also mit Einwilligungen zur Legitimation der Datenverarbeitung gearbeitet werden.
[x] Vgl. Erwägungsgrund 42
[xi] Vgl. Art. 7 Abs. (4) DSGVO sowie die Erwägungsgründe 32 und 43
[xii] https://lfd.niedersachsen.de/startseite/themen/wirtschaft/nutzung-von-whatsapp-in-unternehmen-179649.html (abgerufen am 05.11.2020)
[xiii] Vgl.: https://lfd.niedersachsen.de/download/132861/Merkblatt_fuer_die_Nutzung_von_WhatsApp_in_Unternehmen.pdf
[xiv] Als App für Android käme z.B. XPrivacyLua in Frage (vgl. https://lua.xprivacy.eu, abgerufen am 11.11.2020)
[xv] Diese Lösung mag auf der Hand liegen, sie erfordert allerdings eine erhebliche Disziplin der Mitarbeiter und wird kaum im hektischen Betriebsalltag stringent durchzuhalten sein.
[xvi] Solche Lösungen werden u.a. z.B. von Casengo, Messengerpeople, Trengo, Userlike, Zendesk angeboten. Für weitere Informationen rufen Sie die verlinkten Webseiten der Anbieter auf.
[xvii] Vgl. Studie Technologiestandorte Weltweit der Unternehmensberatung Contor aus Hünxe: https://www.thema-standortanalyse.de/e-books-zur-standortanalyse/technologiestandorte-welt/ (abgerufen am 06.11.2020)
[xviii] Vgl. https://telegram.org/faq#f-wo-ist-der-standort-von-telegram (abgerufen am 05.11.2020)
[xix] Oliver Huq, „Die USA sind kein sicherer Hafen mehr", Artikel vom 08.12.2015 veröffentliche in der com!professional, vgl. https://www.com-magazin.de/praxis/datenschutz/usa-sicherer-hafen-1062801.html (abgerufen am 06.11.2020)
[xx] Vgl. u.a.: https://datenschutz.hessen.de/datenschutz/internationales/eu-standardvertragsklauseln; https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/; https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt2/Schutz_der_Persoenlichkeitsrechte/Schutz_der_Persoenlichkeitsrechte.php (alle abgerufen am 05.11.2020)
[xxi] Die EU-Kommission definiert BCR wie folgt: „*Binding Corporate Rules (BCR) sind Datenschutzrichtlinien, die von Unternehmen mit Sitz in der EU bei der Übermittlung personenbezogener Daten außerhalb der EU innerhalb einer Unternehmensgruppe oder eines Konzerns eingehalten werden. Solche Regeln müssen alle allgemeinen Datenschutzprinzipien und durchsetzbare Rechte enthalten, um angemessene Garantien für Datentransfers zu gewährleisten. Sie müssen rechtsverbindlich sein und von jedem betroffenen Mitglied der Gruppe durchgesetzt werden.*" (vgl. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en, abgerufen am 06.11.2020)
[xxii] Vgl. Art. 47 DSGVO
[xxiii] Angaben ohne Gewähr und Garantie auf Vollständigkeit
[xxiv] https://www.ginlo.net/de/business/messenger/pricing/ (abgerufen am 06.11.2020) und auf Anfrage
[xxv] Auf jedem iOS-Device vorinstalliert
[xxvi] Beachten Sie hier insbesondere die von der Datenschutzkonferenz veröffentlichten Hinweise und Muster zum Verzeichnis über Verarbeitungstätigkeiten: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html (abgerufen am 06.11.2020)
[xxvii] https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf (abgerufen am 06.11.2020)