

# Messenger-Dienste im Unternehmen

Ist WhatsApp für die geschäftliche Kommunikation im Unternehmen datenschutzkonform einsetzbar?

von Anna von Laer, Bielefeld



IMAGO / Friedrich Stark

Die Qual der Wahl

Der Messenger-Dienst WhatsApp ist sehr beliebt, einfach bedienbar und bei über 80 Prozent der Smartphonennutzer verbreitet, sodass Vielen der Umgang mit dieser Anwendung vertraut ist. Nicht nur im privaten Rahmen, sondern auch im Unternehmen verspricht WhatsApp einfache Möglichkeiten des Austausches sowohl in der internen als auch in der Geschäftskommunikation. Vielen Unternehmen ist jedoch bewusst, dass der Einsatz von WhatsApp datenschutzrechtliche Probleme nach sich ziehen kann, sodass dass aus Datenschutzgründen häufig eine Nutzung von Seiten der Unternehmensführung untersagt ist, die Mitarbeitenden aber dennoch der Einfachheit halber WhatsApp im Arbeitskontext nutzen. Diese Praxis birgt ein noch größeres Risiko für die IT-Sicherheit und begünstigt Datenschutzverstöße.

Aber was macht die Nutzung von WhatsApp im Unternehmen so riskant? Zum einen handelt es sich bei Messenger-Apps grundsätzlich um ein gesetzlich wenig reguliertes Medium. Die Nutzung solcher Dienste erfolgt über das Internet und ist technisch nicht an einen bestimmten Festnetz- oder Mobilfunkanschluss gebunden, sie werden auch als Over-The-Top-Dienste (OTT Dienste) bezeichnet. Klassische Kontrollmechanismen über das Telekommunikationsgeheimnis wie bei Telefon oder SMS, die im Telekommunikationsgesetz (TKG) verankert sind, gelten hier nicht. Es ist geplant, OTT Dienste über die e-privacy Verordnung stärker zu regulieren, auf das Inkrafttreten dieser Richtlinie wird jedoch bereits seit Jahren gewartet. Bis dahin muss die Nutzung solcher Dienste nach allgemeinen rechtlichen Aspekten geprüft werden.

Bei WhatsApp besteht das Risiko, dass die Betreiber über die Anwendung auf eine Vielzahl personenbezogener Daten wie Nutzerprofile und gegebenenfalls auch Kommunikationsinhalte Zugriff haben. WhatsApp wirbt zwar mit einer Ende-zu-Ende-Verschlüsselung der Kommunikation, wodurch Inhalte nicht durch unbefugte Dritte einsehbar sind. Der Nutzer selbst hat jedoch keinen Einfluss auf die Verschlüsselung und kann somit nicht überprüfen, ob WhatsApp Zugriff auf die Informationen hat. Die Aussage, dass sie als Betreiber keine weiteren Daten auswerten, ist demnach nicht verlässlich überprüfbar. Das birgt zusammen mit der fehlenden Geltung des Telekommunikationsgeheimnisses das Risiko, dass WhatsApp-Metadaten rund um die Nutzer und/oder die Kommunikationsinhalte für eigene, und sogar seit dem Zusammenschluss mit Facebook für konzernweite Zwecke ausnutzt.

Eine weitere datenschutzrechtliche Herausforderung bei der Kommunikation über WhatsApp bleibt aber die Tatsache, dass ein Kontakt nur dann möglich ist, wenn die Mobiltelefonnummern der Gesprächspartner ausgetauscht werden. Grundsätzlich wird bei Installation der App nach der Freigabe des Telefonbuchs gefragt. Allerdings haben bei einer Übermittlung von Adressbüchern die darin enthaltenen Kontakte einer Weitergabe ihrer Daten in der Regel nicht wirksam zustimmen können. Man hat zwar die Möglichkeit, den Zugriff auf das Telefonbuch zu untersagen. Das führt aber dann dazu, dass der Nutzer nur Nachrichten empfangen kann, selbst aber keine Erstkontakte initiieren kann. Dies schränkt die Funktionalität von WhatsApp

natürlich erheblich ein und widerspricht dem Nutzungsprinzip eines Messengers.

Jenseits des Datenschutzes ergeben sich weitere Aspekte, die Unternehmen bei der Nutzung von Messenger-Diensten beachten müssen. Bei geschäftlicher Kommunikation über Vertragsabsprachen zum Beispiel können etwaige gesetzliche Aufbewahrungsfristen – in der Regel 10 Jahre – schwerlich eingehalten werden. Ein Archivierungssystem für Geschäftsbriefe und Emails gibt es für WhatsApp nicht. Hinzu kommt die Tatsache, dass die Kommunikation nicht zentral zu dem entsprechenden Vorgang gespeichert werden kann, sondern sich auf dem Gerät des jeweiligen Mitarbeitenden befindet. In vielen Fällen wird WhatsApp auch ohne geschäftliche Lizenz manchmal sogar über die privaten WhatsApp-Konten der Mitarbeitenden genutzt woraus sich ein lizenzrechtliches Problem ergibt. In den Nutzungsbedingungen von WhatsApp wird in erster Linie die private Kommunikation berücksichtigt, für geschäftliche Kontakte wird die Anwendung WhatsApp-Business angeboten.

Grundsätzlich ist die Nutzung von WhatsApp im dienstlichen Kontext unter den oben genannten Gesichtspunkten kritisch zusehen, auch bei aufgeklärter Nutzung kann ein datenschutzrechtliches Restrisiko und somit auch ein Bußgeldrisiko nicht ganz ausgeschlossen werden kann. Möchte man im Unternehmen dennoch WhatsApp als Messenger-Dienst nutzen, sollte man bestimmte Voraussetzungen dafür schaffen. Dazu gehört zum einen, dass das Unternehmen bei der Nutzung von WhatsApp darauf achten, dass die Kommunikation über geschäftliche Lizenzen und nicht über die Privatgeräte der Mitarbeitenden läuft. Geschäftspartner und Kunden sollten umfassend vorab durch entsprechende Datenschutzhinweise über die Nutzung und Risiken von WhatsApp hingewiesen werden. Auch interne Schulungen der Mitarbeiter und deren Sensibilisierung bei der Nutzung von WhatsApp sind empfohlen. Aufgrund der fehlenden Einwilligung in die automatische Übertragung von Telefonnummern auf die Server von WhatsApp ist es zudem unerlässlich, dass die Initiative zum Erstkontakt vom (informierten) Kunden aus erfolgt. Generell sollte darauf geachtet werden, dass WhatsApp zum Austausch von sensiblen Daten nicht geeignet ist, sondern nur für Informationen, die keiner besonderen Vertraulichkeit unterliegen. Bei einem Austausch über Vertragsinformationen müssten auch die gesetzlichen Speicherfristen beachtet werden und essentielle Informationen separat gespeichert werden.

## Welche alternativen Messenger-Dienste gibt es für Unternehmen?

Unternehmen haben die Möglichkeit, für ihre Kommunikation auch auf andere Messenger-Dienste zurück zu greifen. Einige Herausforderungen, die bei der Nutzung von WhatsApp bestehen, müssen auch bei anderen Messenger-Diensten beachtet werden. Auch bei Anwendung alternativer Dienste muss be-

rücksichtigt werden, dass es sich hierbei um OTT-Dienste handelt, welche gesetzlich wenig reguliert sind und die nicht unter das Telekommunikationsgeheimnis fallen. Dies ist bedeutsam für die Entscheidung, welche Informationen über dieses Medium verschickt werden sollen. Weiterhin gilt auch hier, dass man beim Austausch geschäftlicher Nachrichten die gesetzlichen Speicherfristen berücksichtigen muss. Es gibt jedoch einige Dienste, deren Nutzung im Gegensatz zu WhatsApp ein deutlich geringeres datenschutzrechtliches Risiko bergen.

Der zurzeit bekannteste und beliebteste Dienst ist der Open Source Messenger Signal. Entwickelt wurde er durch die nach US-amerikanischem Recht gemeinnützige Signal Stiftung. Durch die Veröffentlichung des Quellcodes sind die Funktionen und die Sicherheit von Signal – anders als bei WhatsApp – überprüfbar. Die Ende-zu-Ende Verschlüsselung gilt bei Signal nicht nur zwischen den Nutzern, sondern auch gegenüber den Betreibern. Signal hat einen der wichtigsten datenschutzrechtlichen Grundsätze konsequent umgesetzt und stellt sicher, dass die Betreiber durch das „Zero-Knowledge-Prinzip“ keinen Zugriff auf Nutzerdaten haben.

Eine weitere sinnvolle Alternative stellt der Schweizer Dienst Threema dar, der auch Lizenzen speziell für Unternehmen anbietet. Auch Threema legt seinen Fokus sehr auf Datenschutz und kann sogar ohne Angaben der Telefonnummer oder sonstigen personenbezogenen Daten genutzt werden. Die Serverstandorte liegen ausschließlich in der Schweiz, die ein ähnlich hohes Datenschutzniveau wie die EU bietet.

Letztlich ist die Wahl des passenden Messenger-Dienstes auch eine Frage der Verbreitung und der Nutzeranzahl. Wenn ein Dienst im Vergleich zu anderen Diensten weniger Nutzer hat, macht es für Unternehmen im Zweifel keinen Sinn, zu einem unbekannteren Anbieter zu wechseln. Threema zum Beispiel besticht durch seine umfangreiche Datensparsamkeit, ist aber durch die kostenpflichtige Nutzung nicht so weit verbreitet. Dennoch ist hier seit der Ankündigung von WhatsApp, seine Nutzungsbedingungen und weitergehenden Datenaustausch innerhalb des Konzerns zu ermöglichen, ein starker Trend zur Nutzung von Signal und Threema zu beobachten. Das bietet auch Unternehmen die Möglichkeit, datenschutzsichere Messenger-Dienste zu nutzen, die auch eine bedeutende Reichweite bei ihren Kunden und Geschäftspartnern haben.



*Anna von Laer betreut seit dem Frühjahr 2020 als Rechtsanwältin für die MÖNIG Wirtschaftskanzlei Mandate im IT-Recht, Datenschutz- und Gesellschaftsrecht. Sie ist zudem TÜV-zertifizierte Datenschutzbeauftragte. Davor hat sie mehrere Jahre als Justiziarin für eine große Deutsche Stiftung gearbeitet und war dort für die rechtliche Beratung in komplexen IT-Projekten und für die datenschutzrechtliche Umsetzung innovativer Digitalformate zuständig.*

SAVE THE DATE

# Sanierungsberater Jahrestagung

4. und 5. November 2021 | Hybrid-Konferenz in Hamburg

November 2021						
Mo	Di	Mi	Do	Fr	Sa	So
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

**Teilnahmegebühr:**

Abonnenten SanB	269,- €
Behördenvertreter	349,- €
regulär	399,- €

**Rabatte – So sparen Sie intelligent:****Frühbucherrabatt**

5 % bei Buchung bis zum 2. 8. 2021

**Mehrbucherrabatt**

5 % bei Anmelden von 3 oder mehr Teilnehmern einer Institution ab dem 3. Teilnehmer

**Online-Vorteil**

20 % Rabatt auf die Teilnahmegebühr bei Online-Teilnahme

**Anmeldung:**

Frau Maria Belz  
Deutscher Fachverlag GmbH  
Mainzer Landstr. 251, 60326 Frankfurt am Main  
Tel.: +49 69 7595-1157, Fax: +49 69 7595-1150  
E-Mail: Maria.Belz@dfv.de

**Stornierung:**

Die Anmeldung ist übertragbar. Bei Stornierung bis zum 27.9.2021 (Eingangsdatum) wird eine Bearbeitungsgebühr von 75,- EUR zzgl. MwSt. erhoben. Danach ist die volle Teilnahmegebühr zu entrichten.

Der Preis schließt Veranstaltungsunterlagen und die Pausenverpflegung mit ein. Die Teilnahmegebühr bitten wir erst nach Erhalt der Rechnung zu überweisen.

## Anmeldung

Kanzlei/Firma: \_\_\_\_\_

Name, Vorname: \_\_\_\_\_

Position: \_\_\_\_\_

Straße, Nr.: \_\_\_\_\_

PLZ, Ort: \_\_\_\_\_

Tel.: \_\_\_\_\_ E-Mail: \_\_\_\_\_

Abo-Nummer SanB: \_\_\_\_\_

Datum: \_\_\_\_\_ Unterschrift: \_\_\_\_\_

per Mail an [Maria.Belz@dfv.de](mailto:Maria.Belz@dfv.de)  
per Fax an +49 69 7595-1150  
[www.ruw.de/SanB-Jahrestagung](http://www.ruw.de/SanB-Jahrestagung)

**Ja, ich nehme teil:**

- regulär  
 Behördenvertreter  
 als Abonnent SanB
- vor Ort       per Livestream

**Sie haben den SanB noch nicht im Abo?**

- Ich möchte den SanB Sanierungsberater zum Jahresbezugspreis Inland für 229,-€ (inkl. Vertriebskosten und MwSt.) abonnieren und zum Vorzugspreis teilnehmen. Bitte liefern Sie ab sofort.

