# Sichere Messenger für Behörden

Von Dipl.-Jur. Niklas Mühleis, LL.M., Heidrich Rechtsanwälte

An einem Messenger-Dienst auf dem Diensthandy führt heute fast kein Weg mehr vorbei. Seit jedoch bekannte Dienste wie WhatsApp in die Kritik geraten sind, stellt sich die Frage, inwiefern das Verwenden eines Instant Messengers eine Verletzung von Datenschutzregeln darstellen kann. Denn gerade für Ämter und Behörden gilt: Der verwendete Dienst muss den Vorgaben der Datenschutzgrundverordnung (DSGVO) entsprechen.

# Auf einen Blick



# K.o.-Kriterien Datenschutz und Sicherheit

Bei einer ersten Einschätzung der Dienste hilft die Faustregel des Datenschutzes: „Jede Erhebung oder Verarbeitung von Daten bedarf der Zustimmung der betroffenen Personen.“ Je weniger Daten ein Messenger von sich aus erhebt, desto besser ist es grundsätzlich, da der Messenger dann weniger Angriffsfläche für mögliche Datenschutzverstöße bietet. WhatsApp beispielsweise greift auf sämtliche Telefonnummern in der Kontaktliste zu und gleicht auf seinen Servern ab, ob sie ebenfalls einem WhatsApp-Account zugeordnet sind. Was harmlos klingt, ist jedoch eine Datenerhebung ohne Zustimmung der betroffenen Nummerninhaber und somit nicht DSGVO-konform. Das händische Hinzufügen von Kontakten wie bei Microsofts Videotelefoniedienst Skype ist hingegen unproblematisch. Hier gibt es keinen automatischen Abgleich von Kontaktdaten, die Kontaktaufnahme findet zielgerichtet zwischen den Nutzern statt.

Im Bereich der IT-Sicherheit gilt, dass verhältnismäßig sicher kommuniziert werden kann, wenn die Kommunikation durch den Messenger direkt verschlüsselt wird. Zu bevorzugen ist dabei stets eine Ende-zu-Ende-Verschlüsselung, also eine direkte Verschlüsselung der Kommunikation. Selbst wenn diese durch Dritte abgefangen würde, wäre sie nicht lesbar und müsste mit großem Aufwand entschlüsselt werden. Ein Minimum an Datenspeicherung in Clouds erhöht ebenfalls die Datensicherheit. Umfangreiche Datensätze auf externen Servern machen diese hingegen interessant für Hackerangriffe. Einige Messenger-Dienste wie Telegram, welche die Kommunikation auf Servern speichern, verschlüsseln diese Daten zumindest in der Cloud und sorgen so für einen größeren Schutz trotz Cloud-Speicherung.

# Fünf Messenger aus Behördensicht

## WhatsApp

Bei WhatsApp dürfte es sich um die derzeit meistbenutzte Messenger-App handeln. Der Dienst hat damit den Vorteil, dass sein Interface auf Android, iOS und dem Desktop den meisten Usern bereits bekannt ist. Doch damit hören die Vorteile auch schon auf. WhatsApp gehört zum Facebook-Konzern und übermittelt sämtliche auf dem Handy gespeicherten Kontaktdaten an Server in die USA, was einen Verstoß gegen die DSGVO darstellt. Zuletzt hatte die App sogar für Verstimmungen innerhalb der niedersächsischen Landesregierung gesorgt.

Auch in puncto IT-Sicherheit gibt es Mängel. Ende letzten Jahres wurde eine gravierende Sicherheitslücke im Code von WhatsApp aufgedeckt, über die sich ganze Handys hacken ließen.

## iMessage

Apples hauseigener Messaging-Dienst, der damit nur für iOS verfügbar ist, heißt iMessage. Auch wenn der Dienst nicht ans iPhone gebunden ist, sondern die Nachrichten auch auf dem Mac abgerufen werden können, dürfte er dadurch für die meisten Verwaltungen uninteressant sein.

Der Dienst iMessage bietet die üblichen Features wie Gruppenchats und Sprachnachrichten. Apple wirbt mit einer Ende-zu-Ende-Verschlüsselung der Kommunikation, was den Dienst verhältnismäßig sicher macht, und mit der Beachtung der DSGVO. Im Jahr 2016 wurde eine Schwachstelle im Code des Messengers entdeckt, womit Dritten der Zugriff auf dem gesamten Nachrichtenverlauf ermöglicht wurde. Seit deren Behebung wurden keine weiteren Schlupflöcher in der Sicherheitsstruktur bekannt.

## Telegram

Telegram ist kostenlos für Android und iOS verfügbar und lässt sich auch über eine Desktop-App oder den Browser nutzen. Die Nachrichten werden über eine Cloud synchronisiert und können damit auf jedem Gerät parallel abgerufen werden. Davon ausgeschlossen sind die sogenannten „geheimen Chats“, die durch eine Ende-zu-Ende-Verschlüsselung gesichert sind und nach einer Weile automatisiert gelöscht werden.

Hinsichtlich der Umsetzung der DSGVO hat der Dienst in den letzten Jahren ordentlich nachgebessert, allerdings werden auch hier die Kontakte im Telefonbuch mit der Cloud synchronisiert; die Funktion lässt sich aber abschalten, danach können Kontakte nur noch von Hand hinzugefügt werden. Ist dies mit den Inhabern der entsprechenden Nummern abgesprochen, darf die Nutzung als DSGVO-konform gelten; allerdings macht ein solches Vorgehen viel Arbeit.

Anfang 2019 gab es bei Telegram eine Sicherheitslücke, durch die Malware auf Smartphones und PCs eingeschleust werden konnte. Sämtliche Chats und Nutzerdaten werden auf den Telegram-Servern verschlüsselt gespeichert und sind sogar dem russischen Geheimdienst FSB „zu sicher“.

## Threema

Threema ist ein kostenpflichtiger Messenger, verspricht jedoch für die einmalige Gebühr von 3 Euro maximale Sicherheit. Die üblichen Funktionen wie Einzelchats und Gruppen stehen auch hier auf Android und iOS zur Verfügung. Sämtliche Chats, Datenpakete, Sprachnachrichten und Anrufe werden Ende zu Ende verschlüsselt. Die fehlende Cloud-Synchronisierung sorgt für noch mehr Datensicherheit, da es keinen zentralen Server gibt, der Ziel von Hackerattacken werden kann. Das Vertrauen in die Sicherheit des Dienstes aus der Schweiz ist bei der landeseigenen Verwaltung so groß, dass diese den Messenger offiziell auf Diensthandys nutzt.

Über Sicherheitslücken ist bislang nichts bekannt. Die Kontaktsynchronisation muss vor dem ersten Start der App freigegeben werden. Damit gilt Threema als DSGVO-konform.

Der Messenger Threema ist kostenpflichtig, gilt aber als sicher und wird sogar in der Schweizer Bundesverwaltung eingesetzt

## Signal

Signal ist eine kostenfreie App, die als Open-Source-Software ihren Quellcode offengelegt hat. Ähnlich wie bei Threema gibt es für jeden Chat eine Ende-zu-Ende-Verschlüsselung und keine Cloud-Speicherung. Per individueller Einstellung werden Nachrichten nach einem bestimmten Zeitraum automatisch gelöscht. Der Dienst ist für Android und iOS verfügbar und kann auch über eine Desktop-Anwendung genutzt werden. Die üblichen Messenger-Funktionen wie Gruppenchats, Sprachnachrichten und Dateiversendungen sind auch hier vorhanden.

Aufgrund der verschiedenen ineinandergreifenden Sicherheitsvorkehrungen ist Signal als extrem sicher zu bewerten. Zudem orientiert sich Signal grundsätzlich an dem Prinzip der Datensparsamkeit und gilt ebenfalls als DSGVO-konform.

Signal (vormals Textsecure) ist der kostenfreie Messenger, den u.a. Edward Snowden verwendet

# Threema und Signal sind gute Lösungen

Darf WhatsApp aufs Diensthandy? Die Antwort lautet eindeutig nein, der Dienst ist weder besonders sicher, noch entspricht er den Anforderungen an den Datenschutz. Auf Instant Messenger müssen Mitarbeiterinnen und Mitarbeiter von Ämtern und Behörden dennoch nicht verzichten: Mit den Diensten Threema und Signal gibt es eine kostenpflichtige und eine kostenlose Alternative. Beide Dienste sind sehr sicher und werden den Anforderungen der DSGVO gerecht.

# Nützliche Links

- DSGVO-Aktualisierung
- Kryptografie ohne Hintertür
- Mobile Security für Behörden
- Privacy Top 20
- SecurePIM Office

Dipl.-Jur. Niklas Mühleis, LL.M., ist bei der Heise-Kanzlei Heidrich Rechtsanwälte in Hannover tätig, ist spezialisiert auf IT- und IP-Recht sowie außerdem Fachautor für c't und bei insidas.

Heidrich Rechtsanwälte, Vahrenwalder Straße 255, 30179 Hannover, Tel.: 0511-37498150, muehleis@recht-im-internet.de, www.recht-im-internet.de

Quelle: https://www.mittelstandswiki.de/wissen/E-Government:DSGVO-konforme_Instant_Messenger

Zuletzt bearbeitet am 4. Juni 2019. Erstveröffentlichung am 29. April 2019.