WhatsApp?
oder Alternativen?

Trotz immer wieder aufkommender Bedenken wegen des Datenschutzes ist WhatsApp die meistgenutzte Messenger-App in Deutschland. 2023 wurde er laut einer Umfrage des Statistik-Dienstes Statista von 86 Prozent aller Messenger-Nutzer:innen in Deutschland verwendet. Seit 2014 gehört WhatsApp zum Konzern Meta. Der sorgte 2016 (damals noch unter dem Namen Facebook) für einen breiten Aufschrei, als er sich das Recht einräumte, Nutzerdaten von WhatsApp mit allen anderen Diensten des Konzerns austauschen zu dürfen. Dazu gehören zum Beispiel Account-Informationen (u.a. Profilname, Profilbild, Info, Handynummer und ggf. E-Mail-Adresse), es können aber auch Telefonnummern aus Adressbüchern auf dem Smartphone der Nutzer:innen sein. So könnte Meta an noch mehr Daten von Personen kommen, die gar keine Dienste wie zum Beispiel Facebook, Instagram oder Oculus nutzen.
Dem Unternehmen wurde nachgesagt, Nutzerdaten aus WhatsApp auch für die Auswahl interessenbezogener Werbung einsetzen zu wollen – z.B. auf Internetseiten sowie bei Facebook und Instagram. Entsprechende Änderungen der Nutzungsbedingungen haben zum Rechtsstreit mit Behörden und Verbänden geführt. Wegen einer Strafe der irischen Datenschutzbehörde im September 2021 hat WhatsApp die Datenschutzhinweise komplett überarbeitet. Die für Deutschland geltende Version enthält aktuell keine Informationen dazu, dass Nutzerdaten zu Werbezwecken verwendet würden. Gleichwohl erhebt und verarbeitet WhatsApp zahlreiche personenbezogene Daten und gilt daher nicht gerade als datenschutzfreundlicher Messenger-Dienst.
Neben SMS und E-Mail gibt es auch andere Messenger-Apps als Alternative zu WhatsApp. Wir empfehlen generell solche Messenger zu verwenden, die weder Nachrichteninhalte noch andere Daten ihrer Nutzer:innen zu Werbezwecken speichern und analysieren oder weitergeben.

Wichtige Begriffe erklärt

Was heißt Ende-zu-Ende-Verschlüsselung?

Wenn ein Chat Ende-zu-Ende verschlüsselt ist, können nur die Teilnehmer:innen dieses Chats auf die Inhalte zugreifen. Wenn eine Verschlüsselung zuverlässig umgesetzt wurde, können App-Betreiber nicht mitlesen und die Daten auch nicht an Dritte herausgeben.

Es gibt auch Transportverschlüsselung. Dabei werden Nachrichten zwar während der Übertragung zwischen den Geräten der Nutzer:innen und dem Server der App-Betreiber verschlüsselt, aber auf dem Server und den Geräten möglicherweise unverschlüsselt oder mit einem eigenen Schlüssel gespeichert. Betreiber könnten die verschickten Inhalte also (theoretisch) sehen.

Was sind Metadaten?

Als Metadaten bezeichnet man Daten, die Informationen über andere Daten enthalten. Bei Messengern sind Metadaten zum Beispiel folgende Informationen:

Wann wurde eine Nachricht geschrieben und verschickt?

An wen wurde die Nachricht geschickt?

Wann wurde die Nachricht geöffnet?

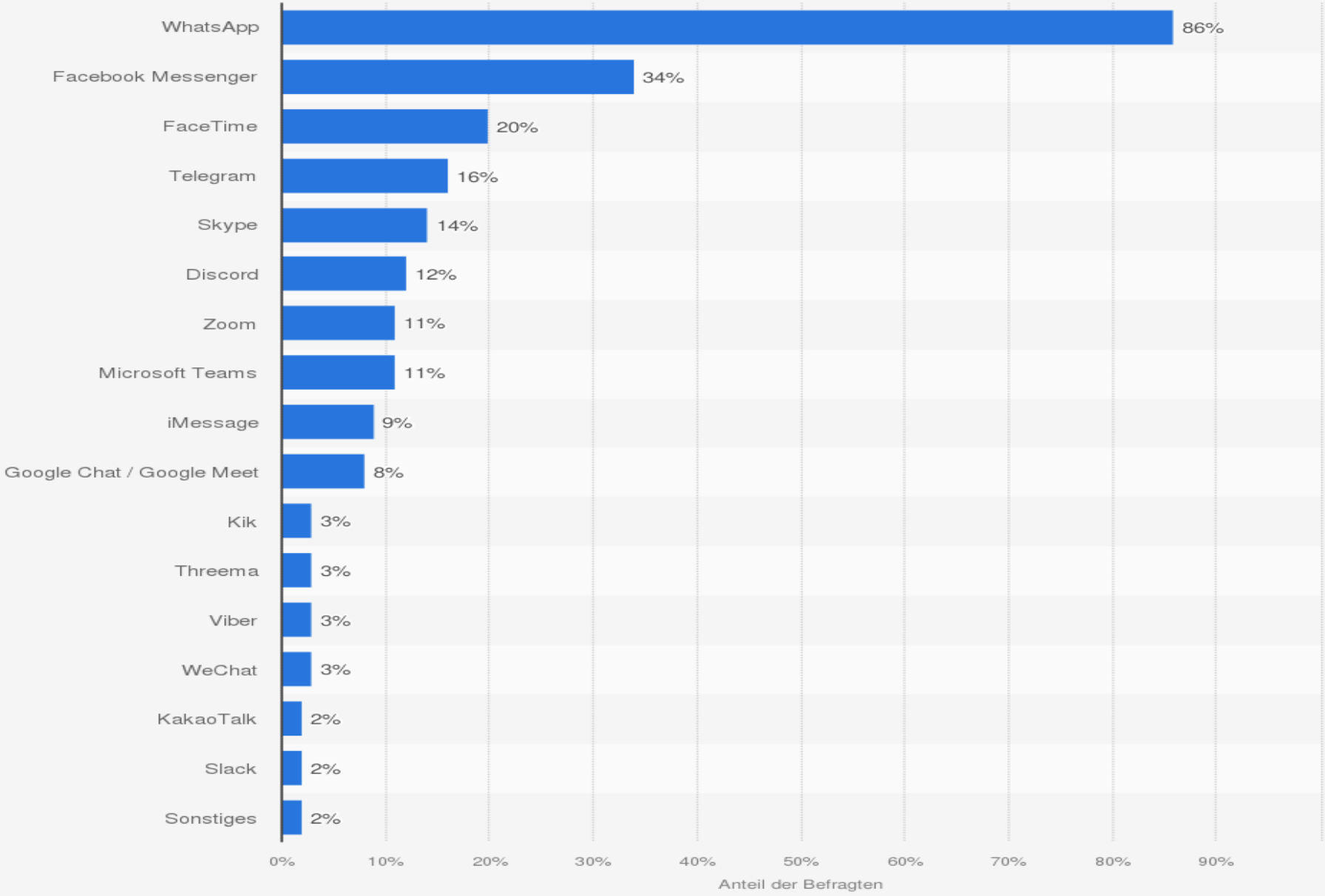
Wie groß war der Inhalt der Nachricht?

Welchen Personen schreibt man wie oft?

Welche Messenger wir uns angesehen haben – und welche nicht

Wir haben uns Anfang 2024 verschiedene Messenger-Apps diverser Anbieter angesehen und grundlegende Funktionen sowie Aussagen der Betreiber zum Datenschutz verglichen. Dabei haben wir nur Apps berücksichtigt, die
für die am stärksten verbreiteten Betriebssysteme (iOS und Android) verfügbar sind,
zum Zeitpunkt des Tests in den offiziellen Stores für Android und iOS verfügbar waren,
als reine Messenger gelten (also keine Apps mit zusätzlicher Nachrichtenfunktion wie Instagram oder TikTok oder Meeting-Software wie Discord, Zoom, Microsoft Teams, Google Meet),
Ende-zu-Ende-Verschlüsselung mindestens einstellbar anbieten und
gemessen an der Nutzerzahl möglichst eine gewisse Verbreitung in Deutschland erreicht haben oder deren Betreiber ihren Firmensitz in Deutschland haben.

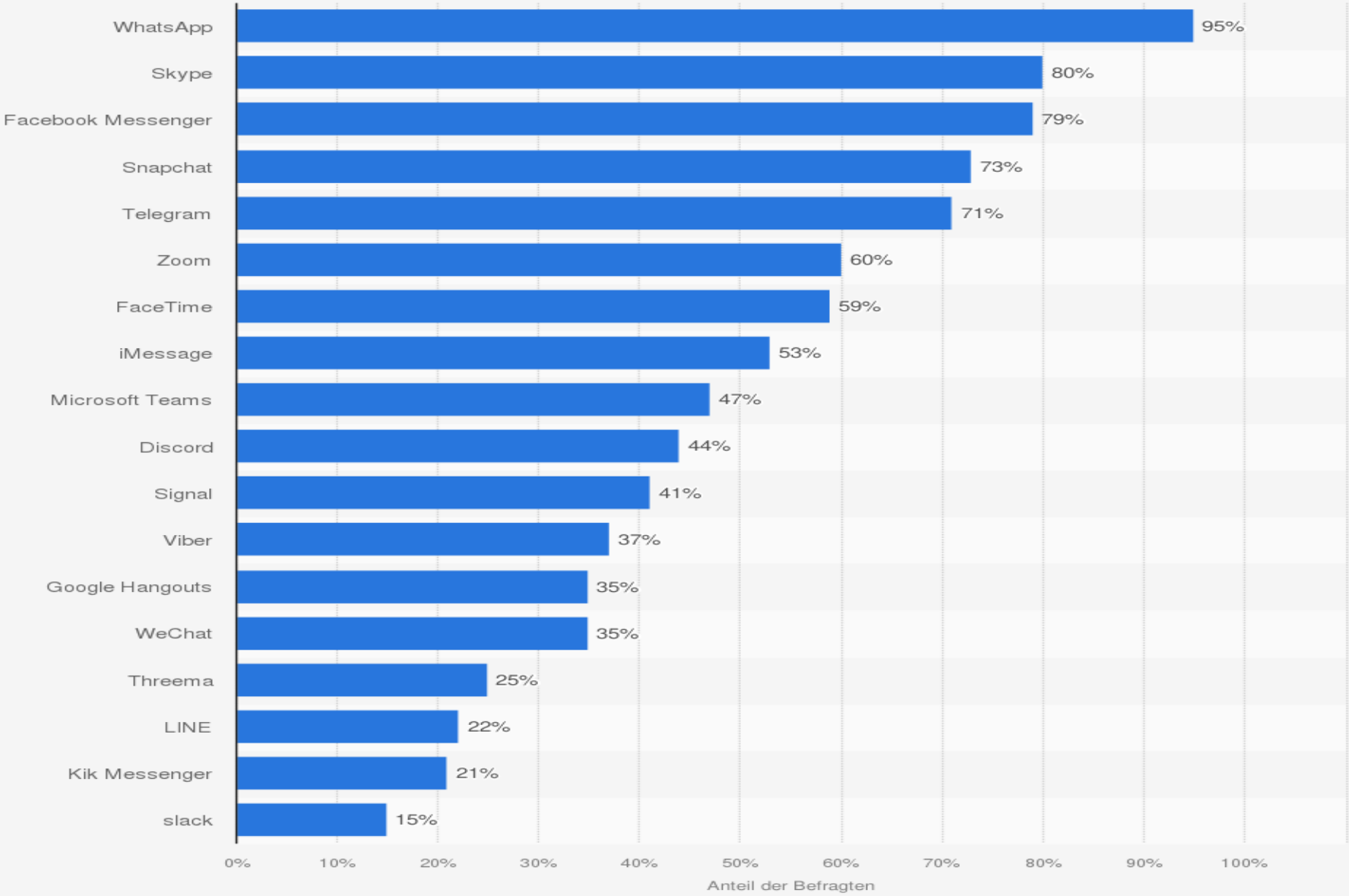
Beliebteste Messenger in Deutschland im Jahr 2023



Quelle
Statista Consumer Insights

Weitere Informationen:
Deutschland; Januar bis Dezember 2023; 4.063 Befragte; 18 bis 64 Jahre; Befragte, die regelmäßig Instant-Messenger n

Ranking der wichtigsten Messenger-Dienste in Deutschland nach Markenbekanntheit im Jahr 2023



Quelle
Statista Consumer Insights

Weitere Informationen:
Deutschland; 06.06.2023; 1.242 Befragte; 18 bis 64 Jahre; Online-Umfrage

Die vor allem bei Jugendlichen beliebte App Snapchat fällt raus, weil sie keine Ende-zu-Ende-Verschlüsselung anbietet. Keine Angaben dazu konnten wir zu den Diensten Google Chat, Kik und WeChat finden, wodurch sie ebenfalls ausscheiden. Nachrichteninhalte könnten ohne Verschlüsselung zum Beispiel vom Anbieter oder unbefugte Dritte gelesen werden. Der Ende-zu-Ende-verschlüsselte
Dienst iMessage ist zwar weit verbreitet, aber nur für Apple-Geräte verfügbar – ebenso wie FaceTime.
Nicht berücksichtigt haben wir Aspekte zur Handhabung, zum Beispiel: Wie schnell ist die App und wie stabil sind die Server? Wie nutzerfreundlich ist die App im Detail gestaltet?
Wir haben uns somit bei Facebook-
Messenger, KakaoTalk, Signal, Skype, Telegram, Threema, Viber und WhatsApp angeschaut, was die Anbieter in ihren Datenschutzbestimmungen und auf ihren Internetseiten zum Hinterlassen von Datenspuren sagen (Stand März 2024)

Weitgehend anonym nutzbare Messenger

Bei der Frage nach einer möglichst anonymen Nutzung geht es an dieser Stelle nicht darum, ob Sie gegenüber anderen Nutzenden anonym bleiben können, sondern ob das auch gegenüber dem Anbieter möglich ist. In unserem Vergleich sind Ginlo und Threema die einzigen Messenger, die ohne eigene personenbezogene Angaben wie E-Mail oder Handynummer einsatzfähig sind.

Ginlo

Existiert seit 2019 als Nachfolger der Messenger-App SIMSme der Deutschen Post. Die ginlo.net Gesellschaft für Datenkommunikationsdienste mbH sitzt in München und schreibt in der Datenschutzerklärung, keine Daten an Server außerhalb des Europäischen Wirtschaftsraums zu übertragen. Zur Nutzung muss nur ein Anzeigename angegeben werden, der auch ein Emoji sein kann. Zugriff auf gespeicherte Kontakte ist möglich, aber nicht zwingend erforderlich. Ende-zu-Ende-Verschlüsselung ist Standard. In jedem Chat kann für einzelne Nachrichten separat die Selbstzerstörung in mehreren Zeitstufen gewählt werden. Nachträgliches Löschen verschickter Nachrichten ist auch möglich – allerdings werden die Nachrichten nicht bei Empfänger:innen gelöscht, sondern nur im eigenen Chat.

Threema

Threema ist der einzige kostenpflichtige Messenger in unserem Vergleich. Wenn Sie sich neu anmelden, erhalten Sie eine zufällig generierte ID, mit der Sie für andere angezeigt werden und sich mit anderen vernetzten können. Alle weiteren Informationen, wie Ihren Namen und ein Profilbild, können Sie freiwillig zusätzlich angeben. Der Anbieter Threema GmbH mit Sitz in der Schweiz hat keine ausufernde Datenschutzerklärung in Bezug auf den Messenger. Er beschreibt viele datenschutzrechtliche Aspekte auf den Hilfeseiten. Demnach speichert Threema nach eigener Angabe Ihre Telefonnummer und/oder E-Mail-Adresse nur auf Wunsch und jeweils verschlüsselt ("gehasht") auf eigenen Servern, um das Auffinden und die Identifizierbarkeit zu erleichtern. Außerdem können die Telefonnummern bzw. E-Mail-Adressen Ihrer Kontakte abgeglichen werden, um Freunde zu finden. Hierzu werden die Daten aus dem eigenen Adressbuch nicht dauerhaft gespeichert, sondern es erfolgt ein Abgleich über einen temporären Hash (eine Verschlüsselungs- bzw. Pseudonymisierungs-Technik). Threema bekommt das Adressbuch mit E-Mail-Adressen und Telefonnummern von Freunden also nur anonymisiert und verspricht, sie zu keinem Zeitpunkt auf einen Datenträger zu speichern.

Selbstlöschende Nachrichten gibt es nicht. Einzelne Nachrichten können nach dem Absenden wieder gelöscht werden, verschwinden aber nur auf dem eigenen Gerät. Auch bei Threema ist die Ende-zu-Ende-Verschlüsselung in allen Chats Standard.

Messenger mit Nutzerregistrierung

Facebook-Messenger

Der Messenger war viele Jahre das Nachrichtensystem der Social-Media-Plattform Facebook. Inzwischen kann er auch ohne ein Facebook-Profil verwendet werden. Dann werden entweder eine Handynummer oder eine E-Mail-Adresse für die Registrierung benötigt. Andere Nutzer:innen können Sie möglicherweise an Ihrem Namen erkennen – in seinen Nutzungsbedingungen verlangt Facebook die Angabe des echten Namens in Profilen. Das darf es nach zwei Urteilen des Bundesgerichtshofs (BGH) vom Januar 2022 nicht mehr pauschal machen (Az. III ZR 3/21 und III ZR 4/21). Den Zugriff auf gespeicherte Handykontakte fordert der Messenger zwar an, er kann aber auch ohne diese Erlaubnis genutzt werden. Für Ende 2023hatte Meta standardmäßige Ende-zu-Ende-Verschlüsselung für Chats mit anderen Personen angekündigt. Doch auch bei unserer Betrachtung im April 2024 war eine Ende-zu-Ende-Verschlüsselung noch kein Standard, sondern konnte durch Start eines "geheimen Chats" eingeschaltet werden. Bei Business-Chats (also beispielsweise dem Nachrichtenaustausch mit Facebook-Seiten von Unternehmen) ist keine durchgehende Verschlüsselung verfügbar. Gruppenchats und (Video-)Telefonate sollen laut Betreiber Meta bereits seit Januar 2022 Ende-zu-Ende verschlüsselt sein.

Betreiber des deutschen Facebook-Messengers und des Netzwerks Facebook ist die Meta Platforms Ireland Limited. Facebook gibt in seiner Datenschutzerklärung an, dass gesendete und empfangene Nachrichten "einschließlich ihrer Inhalte" erfasst werden. Dazu gehöre auch der Nachrichtenaustausch bzw. das Kommunizieren mit anderen. Verwirrend ist allerdings, dass Meta in der Datenschutzerklärung auch angibt, die Inhalte nicht einsehen zu können. Die gesammelten Informationen verwendet Facebook nach eigenen Angaben unter anderem für die Auswahl von Werbung, die auf die Nutzerinteressen ausgerichtet ist. Hier besteht also die gleiche Kritik wie an WhatsApp: Auch wenn Meta angeblich nicht auf Chat-Inhalte zugreifen kann, gibt es immer noch so genannte Metadaten, die ebenfalls zur Bildung von Nutzerprofilen und Personalisierung von Werbung und Inhalten genutzt werden können.

KakaoTalk
Betreiber des Messengers ist die koreanische KaKao Corporation. Die Ende-zu-Ende-Verschlüsselung lässt sich aktivieren, indem Sie einen sog. geheimen Chat starten.
Die Datenschutzerklärung gibt es nicht in deutscher Sprache. Ohne Telefonnummer funktioniert der Messenger nicht. Auf Android verweigert die App auch ihren Dienst, wenn Sie ihr den Zugriff auf gespeicherte Kontakte verwehren. Auf iPhones hingegen funktioniert sie auch ohne Kontaktzugriff. Nachrichten können Sie nicht von selbst verschwinden lassen, aber nach dem Senden für alle im Chat löschen.
Auffällig: Wir konnten unsere beiden Test-Accounts nicht löschen, weil sie – ohne erkennbaren Grund – angeblich gegen die Nutzungsbedingungen verstoßen haben.

Signal
Wenn Sie Signal nutzen möchten, kommen Sie um die Angabe Ihrer Telefonnummer nicht herum. Auch ein Eintrag bei Vorname wird verlangt – hier gibt sich der Messenger aber auch mit der Angabe eines Pseudonyms oder sogar mit einem Emoji zufrieden. Neu hinzugekommen ist Anfang 2024 der Nutzername, der keine Pflicht ist. Sie können ihn als Alternative zur Telefonnummer verwenden, um sich im Messenger mit Personen zu verbinden, denen Sie Ihre Handynummer nicht nennen möchten. Angezeigt wird der Nutzername in Signal-Chats aber nicht.
Erlauben Sie den Zugriff auf die Kontakte Ihres Telefons nicht, müssen Sie die Telefonnummer neuer Chat-Partner:innen oder den Nutzernamen per Hand eintippen. Alle Chats sind standardmäßig Ende-zu-Ende verschlüsselt. Anbieter Signal Messenger LLC. stellt keine Datenschutzerklärung auf Deutsch zur Verfügung. Das Unternehmen sitzt in den USA. Das Verschwinden einzelner Nachrichten kann pro Chat in unterschiedlichen Zeitstufen aktiviert werden und gilt dann für alle künftigen Nachrichten in diesem Chat, bis eine andere Zeit eingestellt oder die Funktion abgestellt wird.

Skype

Um Skype nutzen zu können, benötigen Sie ein Konto bei Microsoft. Denn die Skype Communications SARL in Luxemburg gehört zu Microsoft. Für das Konto sind eine E-Mail-Adresse oder eine Handynummer erforderlich. Sie können sich auch eine E-Mail-Adresse von Microsoft einrichten lassen. Ob andere Skype-Nutzer:innen Ihre personenbezogenen Daten zu Gesicht bekommen, können Sie einstellen. Ende-zu-Ende-Verschlüsselung gibt es nur, wenn Sie eine "private Unterhaltung" führen. Die steht ausschließlich für einen Chat mit einer weiteren Person und nicht für Gruppen zur Verfügung. Private Chats sind auch nur auf den Geräten zu lesen, mit denen sie gestartet werden. Die Inhalte der normalen und damit nicht Ende-zu-Ende verschlüsselten Chats werden von Skype auf Servern gespeichert, um auf mehreren Geräten angezeigt werden zu können. Allerdings geht Microsoft weder in der Datenschutzerklärung noch in der Skype-Hilfe explizit darauf ein, wie diese Daten gespeichert werden (ob verschlüsselt oder nicht) und wo die entsprechenden Server stehen.
Selbstlöschende Nachrichten gibt es nicht. Aber Sie können bereits gesendete Nachrichten löschen, die dann auch bei den anderen Chat-Partner:innen entfernt werden.

Telegram

Die Telegram Messenger Inc. stellt seine Datenschutzerklärung in deutscher Sprache zur Verfügung. Nachdem der Firmensitz viele Jahre verschwiegen wurde, wird in der Datenschutzerklärung nun eine Anschrift auf den Britischen Jungferninseln genannt. Neben der zwingenden Notwendigkeit der Verknüpfung mit der Telefonnummer fordert die App die Angabe eines Namens, der auch ein Pseudonym sein kann. Ob andere Nutzer:innen Ihre Telefonnummer, Profilbilder, den Online-Status oder die Biographie sehen können, können Sie einstellen. Auch die Weiterleitung Ihrer Nachrichten durch andere, die Anrufmöglichkeit innerhalb der App und die Möglichkeit zur Einladung in Gruppenchats können in den Einstellungen geregelt werden.
Wie bei Skype kann man auf Telegram-Chats mit verschiedenen Geräten zugreifen. Dafür sind die Chat-Inhalte auf Servern von Telegram gespeichert. Nach Anbieterangaben sind sie dort lediglich einfach verschlüsselt. Wem das nicht ausreicht, der kann eine Ende-zu-Ende-Verschlüsselung aktivieren bzw. die "Geheimen Chats" verwenden, bei denen die Nachrichten Ende-zu-Ende verschlüsselt werden. Deren Inhalte werden laut Telegram nur auf den Geräten der Teilnehmenden, also nicht mehr in einer Cloud, gespeichert. Beim Deinstallieren der App oder einem Gerätewechsel sind die eingegebenen Inhalte dann aber weg. "Geheime Chats" stehen nicht für Gruppengespräche zur Verfügung.
Telefonnummern sowie Vor- und Nachnamen von Kontakten aus dem Adressbuch werden gespeichert, wenn die Kontaktsynchronisation genutzt wird. Ohne Zugriff auf das Adressbuch ist – anders als bei Android – bei iOS kein Start eines Chats möglich. Die Synchronisation kann an- und abgeschaltet werden und synchronisierte Kontakte können von den Telegram-Servern gelöscht werden. Bei Inaktivität von wahlweise 1, 3 oder 6 Monaten bis zu einem Jahr wird das Nutzerkonto automatisch gelöscht. Der Zeitraum lässt sich in den Einstellungen ändern. Das automatische Verschwinden einzelner Nachrichten kann mit unterschiedlichen Zeitstufen aktiviert werden und wirkt sich dann auf alle künftigen Nachrichten in Chats aus.