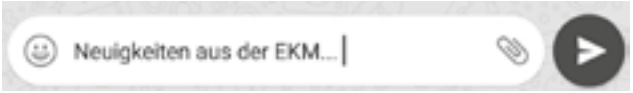
# WhatsApp datenschutzkonform?
## Ja, mit etwas Aufwand, aber es geht.

BEILAGE MÄRZ 2019

Die unbedarfte Nutzung von WhatsApp ist datenschutzrechtlich problematisch. Sei es der firmeninterne Datenabgleich mit Facebook, die unsichere bzw. nicht durchgängige Verschlüsselung oder die Datenverarbeitung außerhalb der EU. Diese Mängel nehmen wir wahr. Auch das Quasi-Monopol und die daraus resultierenden Abhängigkeiten sehen wir kritisch. Da WhatsApp alle Telefonnummern des Adressbuches mit den Servern in den USA abgleicht, dürfen im Adressbuch des Telefons streng genommen nur Nummern von Personen stehen, die dieser Datenübermittlung dem Nutzer gegenüber ausdrücklich zugestimmt haben. Die meisten Nutzerinnen und Nutzer haben diese Zustimmung nicht von allen im Adressbuch Eingetragenen eingeholt. Gleichwohl lässt sich WhatsApp diese Zustimmung vom Nutzer zusichern. Aus Sicht des Datenschutzes ist die WhatsApp-Nutzung rechtlich nur in engen Grenzen zulässig. Die Situation ist unübersichtlich, da eine eindeutige, übergreifende Bewertung von WhatsApp etwa durch die staatlichen Datenschutzbeauftragten noch aussteht. Manche Unternehmen verbieten mittlerweile die Nutzung von WhatsApp für dienstliche Zwecke.

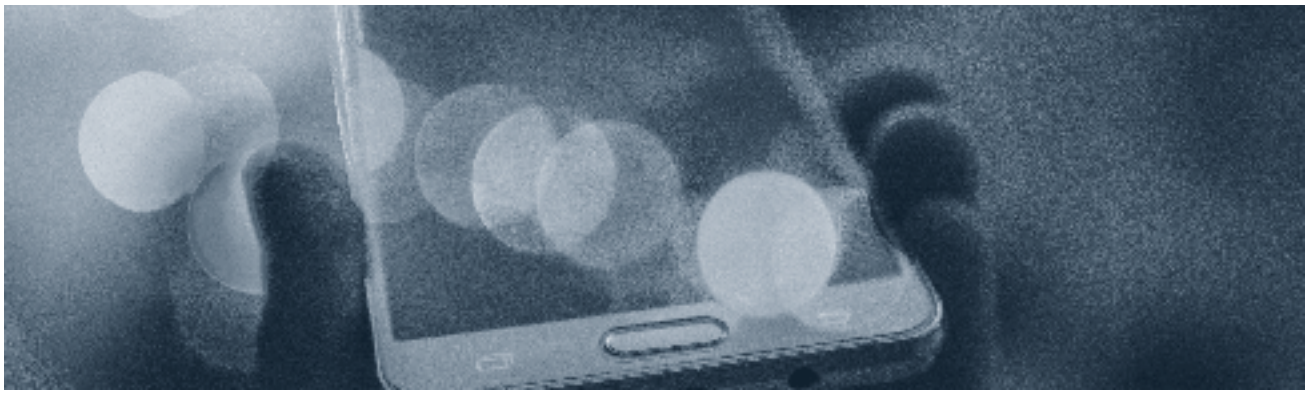
Der Datenschutzbeauftragte der EKD rät vom Einsatz ab (Stellungnahme vom 24. Oktober 2018).

Gleichzeitig sehen wir, dass viele Menschen in der EKM diesen Messenger nutzen, darunter auch viele kirchliche Mitarbeiterinnen und Mitarbeiter. Gerade bei der Arbeit mit Konfirmanden und Jugendlichen ist eine Kommunikation ohne WhatsApp beinahe undenkbar. Menschen tauschen Texte, Bilder, Videos und Sprachnachrichten aus, in persönlichen Freundeskreisen werden Gruppen-Chats genutzt und per Broadcast-Nachricht werden viele Menschen erreicht, die sich untereinander nicht kennen müssen, aber ein gemeinsames Interesse haben. Diese schnelle und einfache Kommunikation ist trotz aller Kritik weit verbreitet, und für kirchliche Kommunikation wäre es hilfreich, diese Kanäle bespielen zu können.




Bessere Wege wären, für solche Szenarien einen sicheren Messenger zu nutzen, der eine nicht abschaltbare End-zu-End-Verschlüsselung garantiert und unter sauberen Datenschutzbedingungen nutzbar ist. Einige Anbieter versuchen, genau das zu tun. Laut Einschätzung des Datenschutzbeauftragten der EKD sind Threema und SIMSme datenschutzrechtlich unbedenklich. Darüber zu reden und (gerade Jugendliche) für das Thema zu sensibilisieren, ist sowohl medienpädagogisch als auch ethisch sinnvoll. Dennoch sehen wir realistisch, dass in näherer Zukunft weiterhin große Teile der Bevölkerung WhatsApp nutzen werden und daher ein alternativer (kirchlicher) Messenger nur eine Ergänzung sein kann.





## Folgende Szenarien sind derzeit als datenschutzrechtlich unbedenkliche Nutzung von WhatsApp bekannt:

1. Seit Kurzem gibt es für Samsung Smartphones mit Android ab V7.4 die Samsung App „Sicherer Ordner“. Darüber ist es möglich, einen geschützten Bereich des Telefons von anderen abzutrennen. So können private und berufliche Daten auf einem Gerät getrennt verwaltet werden oder eben ein Bereich definiert werden, in dem WhatsApp von den nicht autorisierten Kontaktinformationen getrennt genutzt werden kann.
   Diese Methode ist nur für bestimmte Smartphones anwendbar (Anleitung siehe unten). Es gibt auch für Apple-Geräte ähnliche Insellösungen (Anleitung „Secure Contact“ siehe unten). Es ist allerdings ein wenig Bastelarbeit bzw. eine fundierte IT-Unterstützung nötig.
2. Mit zusätzlichen Apps wie MobileIron, SecureContact oder WhatsVO (Kurzinfos siehe unten) können separate Adressbücher erstellt werden. So kann man die WhatsApp-autorisierten Daten von den nicht freigegebenen trennen und auf einem Gerät beide Datenquellen verwalten.
   Diese Methode kann hilfreich sein, wenn man ohnehin ein Gerät für private und berufliche Belange teilt und damit bestmöglichen Schutz und Sicherheit kombinieren will. Aber auch diese Lösungen erfordern technisches Verständnis und kosten teilweise etwas Geld.
3. Die dritte Möglichkeit ist die pragmatischste und aufwändigste zugleich: Ein separates (ggf. altes und zurückgesetztes) Smartphone ohne personenbezogene Daten wird mit einer günstigen Prepaid-Karte genutzt, um lediglich WhatsApp darüber zu verwenden.
   Das kann zum Beispiel für Gemeinden oder Einrichtungen interessant sein, die ohnehin nur redaktionelle Broadcast-

Nachrichten verbreiten und keine Alltags-Kommunikation anstreben, sodass das Zweitgerät gegebenenfalls auf dem Schreibtisch liegen bleiben kann. Auch bietet sich ein altes, ausgedientes Modell an, wenn man ohnehin die aktive Kommunikation über die Browser-Schnittstelle WhatsApp-Web (Anleitung siehe unten) nutzt (bei der aber dennoch eine Smartphone-Instanz zur Autorisierung benötigt wird).

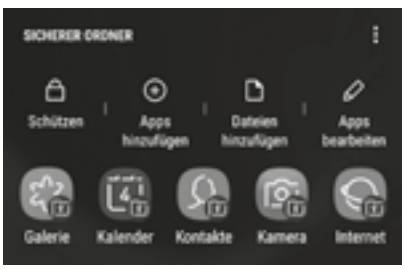
Dahinter fängt die Grauzone an…

---

# Hilfreiche Tools für die datenschutzkonforme Whats-App-Nutzung:

## „Sicherer Ordner“ (Android auf Samsung)

- Im Google Playstore gibt es die (kostenlose) App „Sicherer Ordner“ (Secure Folder), die auf Samsung-Smartphones der Generation 7 und höher nutzbar ist.
- Nach der Installation gibt es einen neuen Container auf dem Smartphone, in dem man unabhängig vom Gesamtgerät Apps installieren und Daten verwalten kann. Es ist zwar möglich, einzelne Inhalte manuell zwischen Gerät und Container hin und her zu schieben, aber grundsätzlich sind die Ebenen getrennt. Das kann zum Beispiel hilfreich sein, um private von beruflichen Daten zu trennen, wenn man ein Gerät für beide Zwecke nutzt. Ebenso kann man WhatsApp im Sicheren Ordner installieren, ohne dass die App Zugriff auf das Haupt-Adressbuch hätte. Die Kontakte, die eine explizite Erlaubnis für die Kommunikation via WhatsApp gegeben haben, kann man dann ins Adressbuch des Sicheren Ordners kopieren und so getrennte Datensätze verwalten.
- tinyurl.com/y8l2q4ac




## „Secure Contact“ (iOS)

- Die App „Secure Contact pro“ bietet für 8,99 Euro einen sicheren Ordner für Apple Smartphones.
- Auch hier wird zwischen Daten in Secure Contact und im Systemadressbuch unterschieden, sodass WhatsApp getrennt von unautorisierten (Geschäfts-)Kontakten nutzbar ist.
- Allerdings muss der Nutzer aktiv entscheiden, welche Kontakte in welches Adressbuch gespeichert werden.
- tinyurl.com/y8uk37m7

## „Mobile Iron“

- Wer als Unternehmen oder Einrichtung mehrere Mobiltelefone managen möchte, kann das (kostenpflichtige) Management-Tool von MobileIron verwenden. Auch damit ist es möglich, einen sicheren Container zu verwenden, um sensible Daten von anderen Inhalten zu trennen.
- Für Endanwender ist MobileIron allerdings nicht ohne Weiteres einsetzbar.

### „Whats VO“

- Unter Android kann die (kostenfreie) App WhatsVO DS-GVO-konform WhatsApp Erlaubnisanfragen verwalten. Dazu schreibt sie den Kontakten im Adressbuch eine Kurznachricht (Achtung, wenn man keine Flatrate hat gegebenenfalls mit Übertragungskosten verbunden!) mit der Bitte um Zustimmung zur WhatsApp-Kommunikation.
- Erst wenn auf diese Anfrage eine positive Reaktion gesendet wird, wird der Kontakt ins WhatsApp-Adressbuch übernommen und kann darüber kontaktiert werden.
- Wir sind als EKM mit den Entwicklern im Gespräch, den Dienst auf kirchliche Belange hin weiter zu optimieren. Es scheint eine einfache Möglichkeit zu sein, um langfristig und legal WhatsApp zu nutzen. Eine Entwicklung der nötigen Erweiterung und finale Einschätzung der App steht allerdings noch aus.
- tinyurl.com/y843dnug

### „WhatsApp-Web“

- Wenn die grundsätzlichen Datenschutzprobleme für ein System gelöst wurden, gibt es die Möglichkeit, den Messenger über eine Browser-Schnittstelle zu nutzen.
- Dazu ruft man die Website web.whatsapp.com auf, scannt den dort erscheinenden QR-Code mit dem Smartphone, auf dem WhatsApp installiert ist, um sich zu autorisieren, und kann dann vom Computer aus mit seinen Kontakten, Listen und Gruppen kommunizieren.
- Zwar greift die Browserversion nicht auf Kontaktinformationen des Computers zu, aber das Telefon, das zur Autorisierung genutzt wird, muss regelmäßig in der Nähe sein und wird als Referenz inklusive Adressbuchdaten genutzt.
- Diese Variante kann genutzt werden, um komfortabel Broadcast-Nachrichten an einen vorher eingerichteten Verteiler zu verschicken und Rückläufe zu verwalten.



## Datenschutzfreundlichere Alternativen zur WhatsApp-Nutzung:

**Alternative Threema:** Ein Schweizer Unternehmen mit strengen Datenschutzrichtlinien und sicherer Ende-zu-Ende-Verschlüsselung. Kontakte werden nicht als Klartext, sondern nur in Form von Hashwerten abgeglichen, um Freunde zu finden. Zwar lässt sich die Firma in puncto Verschlüsselung nicht in die Karten schauen, ist aber aus Datenschutzsicht der aktuell empfehlenswerteste Messenger. Kostet je nach Version 2 bis 4 Euro. Für berufliche Nutzung ist Threema Work zu empfehlen.

- https://threema.ch/de
- tinyurl.com/oeg8t2j
- tinyurl.com/mf7gvdw

**Alternative Signal:** Ein freier und quelloffener Messenger, der sichere Ende-zu-Ende-Verschlüsselung verspricht und dennoch kein Geld kostet. Das macht ihn für manche verdächtig (womit verdient die Firma dann etwas?), andere vertrauen dem Urteil Edward Snowdens, der offen diesen Messenger empfohlen hat. Der EKD-Datenschutz moniert jedoch, dass Daten in den USA verarbeitet werden.

- https://signal.org/
- tinyurl.com/pyu6y32
- tinyurl.com/o4fhy3a

**Alternative SIMSme:** Ein Dienst der Deutschen Post, der sich durch Sicherheit und guten Datenschutz auszeichnet, aber (bisher) noch sehr wenig Nutzer hat. Auch als Business-Version nutzbar.

- https://www.sims.me/
- tinyurl.com/ya4fjc3c
- tinyurl.com/y8sddkvq

**Alternative Jabber:** Jabber ist ein Dienst, der ähnlich wie E-Mail als freier Standard funktioniert, sodass Nutzer ihren Provider selber wählen können. Über das freie Protokoll XMPP (das auch die meisten „großen Anbieter“ nutzen) werden gesicherte Nachrichten ausgetauscht und verbinden Smartphones sowie Computer miteinander. Beliebte Apps, um Jabber auf Smartphones zu nutzen, sind ChatSecure (iOS), Conversations (Android) oder Pidgin (Windows). Durch die Unabhängigkeit von großen Konzernen ist der Dienst unter technikaffinen Nutzern sehr beliebt und mit etwas Hintergrundwissen auch recht einfach einzurichten. Die OnlineKirche der EKM experimentiert mit Jabber als internem Kommunikationskanal und kann auf Anfrage Auskunft zum System und zur Einrichtung von Accounts/Servern geben.

- https://www.jabber.de/was-ist-jabber bzw. https://quicksy.im/
- https://conversations.im/
- tinyurl.com/y9c22y34

## Weitere Stimmen zur Debatte:

- Michael Jakob (EKD-Datenschutz) mit einer generellen Problemanzeige: tinyurl.com/yd3qf49r
- Heiko Kuschel (Citykirche Schweinfurt) kommentiert aus Nutzersicht: tinyurl.com/yab3pdv4
- Die Landeskirche Hannover reagiert mit einem eigenen internen Messenger: tinyurl.com/yd52f32p
- Wolfgang Loest (Lippische Landeskirche) beschreibt das Problem und eine 2-Geräte-Lösung: tinyurl.com/ya538uer
- Lutz Neumeier (EKHN) beschreibt die Nutzung von SecureContact: tinyurl.com/y8o6ct5d
- Ralf-Peter Reimann (EKiR) stellt fundiert und vermittelnd Problem und Lösungsansätze gegenüber: tinyurl.com/y9o4vy6m
- Ergänzende Stellungnahme des EKD-Datenschutzes zu Messengern im Oktober 2018: tinyurl.com/ya8j3eet
- Basics-Podcast von „Kirche digital entdecken“ zum Thema Messenger: tinyurl.com/yb6fzsor


IMPRESSUM

Eine Stellungnahme der Evangelischen Kirche in Mitteldeutschland (EKM)
Erarbeitet durch das Referat Presse- und Öffentlichkeitsarbeit in Absprache mit dem Referat Allgemeines Recht, dem Sachgebiet Informationstechnologie, der Evangelischen Jugend, den Evangelischen Akademien und dem Gemeindedienst.
**Kontakt:** SocialMedia-Koordinator Dr. Karsten Kopjar: karsten.kopjar@ekmd.de, 0361 51800-148