Liste datenschutzfreundlicher Tools (2020)

Alternative Messenger-Dienste

Hoocer

+ Ende-zu-Ende-Verschlüsselung
+ anonym nutzbar
+ lt. Stiftung Warentest 2015 Testsieger bei Messenger in puncto Sicherheit
+ man braucht keine Telefonnummer eingeben
+ NutzerInnen werden über zufälligen Zahlencode zugeordnet
+ Server stehen in Deutschland
+ Nachrichten und Anhänge werden nicht gespeichert
- „In der Nähe Funktion“ – alle Nachrichten und Daten werden an alle Personen in der Umgebung innerhalb der Gruppe geschickt (auch wenn plötzlich neue NutzerInnen hinzukommen)
- „In der Nähe Funktion“: ungefährer Standort wird offenbart
- keine Anrufe möglich

Generiert wird eine zufällige client-ID, Kontakte mit eigenem Adressbuch automatisch synchronisieren ist nicht vorgesehen

Threema

+ end-to-end Verschlüsselung
+ Telefonnummer und/oder (verschlüsselte) Mail-Adresse der BenutzerInnen wird nur auf Wunsch gespeichert
+ anonym nutzbar (keine Registrierung mit persönlichen Daten nötig)
+ Ende-zu-Ende-Verschlüsselung
+ Telefonnummern, E-Mail-Adressen und Kontakte können zwar abgeglichen werden, dabei wird das eigene Adressbuch aber nicht dauerhaft gespeichert
+ Telefonnummern, E-Mail-Adressen und Kontakte werden von anderen werden automatisch nur verschlüsselt an Threema weitergegeben und nicht gespeichert
+ ähnliche Funktionalität wie WhatsApp
+ werbefrei
+ Web- und Desktopversion verfügbar
- Bei Standortbenachrichtigung an andere Personen verwendet Threema Google und verweist auf Google-Datenschutzbestimmungen
- Einmalige Kosten von 2,99 €

Abgleich der Kontaktdaten funktioniert über temporären Hash (eine Verschlüsselungs- bzw. Pseudonymisierungs-Technik). Anders als fast alle Messengerdienste stammt Threema aus Europa (Schweiz), sämtliche Server befinden sich dort. Threema ist nach eigener Aussage zu einhundert Prozent unabhängig und eigenfinanziert.

Wire

+ Ende-zu-Ende-Verschlüsselung
+ Kann auf Smartphone und Rechner genutzt werden
+ dabei werden Nachrichteninhalte zwar in verschlüsselter Form auf Servern zwischengespeichert, bis diese zugestellt sind, werden dann aber wieder gelöscht
+ lässt sich auch ohne Zugriff auf das Adressbuch nutzen

+ Kontakte können freiwillig synchronisiert werden, dabei werden verschlüsselte Telefonnummer n aus dem eigenen Adressbuch verwendet
- lässt sich nicht ohne die Angabe eines Namens und einer Handynummer oder E-Mail-Adresse nutzen.

Der Anbieter behält sich explizit die Datenweitergabe an Dritte unter gewissen Voraussetzungen vor, z.B. im Zusammenhang mit der Durchsetzung der Nutzungsbedingungen oder um seine Rechte zu schützen. Auch weist er auf eine mögliche Weitergabe im Falle eines Unternehmenskaufs hin, der auch zu einer anderen Datenverarbeitung führen könnte. Auf mögliche Drittanbieterdienste z.B. von Youtube oder Spotify wird ebenfalls in der Datenschutzerklärung hingewiesen. Für deren mögliche Datennutzung seien die jeweiligen Anbieter verantwortlich.

Signal

+ Ende-zu-Ende-Verschlüsselung
+ Geben Daten im Normalfall nicht an Dritte weiter
+ Funktion selbstzerstörende Nachrichten
+ die gesamte App ist mitsamt Protokoll Open Source
+ kostenlos
+ ähnliche Funktionalität wie WhatsApp
+ werbefrei
+ Web- und Desktopversion
- benötigt Verknüpfung mit der eigenen Telefonnummer sowie einen Nutzernamen (dieser kann aber auch ein Pseudonym oder Emoji sein)
- keine Datenschutzerklärung auf Deutsch
- Profil wird allen Kontakten im Adressbuch gezeigt
- greift auf Kontakte zu, Fotos,…(siehe Link)

Worauf Signal Zugriff hat: https://support.signal.org/hc/de/articles/360007062172-Signal-Berechtigungen

Signal arbeitet mit derselben Verschlüsselungssoftware wie Telegram, Threema (und teilw. WhatsApp), ist auch Eigentümer derselben. Wird von Sicherheitsexperten und Datenschutzorganisationen empfohlen

Telegram

+ Ende-zu-Ende-Verschlüsselung
+ Synchronisation des Adressbuches kann an- und ausgeschalten werden
+ Bei Inaktivität von sechs Monaten werden die Nutzerdaten automatisch gelöscht.
+ Funktion geheime Chats und selbstzerstörende Nachrichten
+ große NutzerInnenschaft
+ Nutzung lückenlos möglich (PC, Smartphone…)
+ ähnliche Funktionalität wie WhatsApp
+ cloudbasiert
- keine Datenschutzerklärung auf Deutsch
- Ein Vorname muss angegeben werden
- Cloud-Chat: Chatinhalte werden auf Servern gespeichert
- Telefonnummern sowie Vor- und Nachnamen von Kontakten aus dem Adressbuch werden gespeichert (wenn die Kontaktsynchronisation genutzt wird), werden aber nicht an Dritte weitergegeben
- Ohne Zugriff auf das Adressbuch ist kein Chat möglich
- Datenschutz muss manuell aktiviert werden
- wenig transparente Unternehmensstruktur
- Sämtliche Kommunikationsinhalte, mit Ausnahme der geheimen Chats, werden dauerhaft für den Betreiber lesbar auf dessen Servern gespeichert – solange alle an der Konversation beteiligen Nutzer die jeweiligen Nachrichten oder ihre Benutzerkonten nicht löschen

Bei geheimen Chats werden private Gespräche technisch verschlüsselt, sie sind für Dritte nicht zugänglich (auch nicht für Telegram)

YooYuu

+ auf Business-Kommunikation ausgelegt
+ Nutzt die Vorteile von E-Mail, funktioniert aber wie eine Messanger, d.h. es sind themenbezogene Chats
+ Beteiligte können zu Themen chatten und das Thema kann nach Erledigung abgeschlossen werden
+ Features wie z.B.: man kann mit einem Klick aus einer Nachricht einen Termin machen oder ein To-Do und von KollegInnen Bestätigungen anfordern.
+ OrganisatorInnen eines Projekts bestimmen, wer an die Daten kommt, MitarbeiterInnen können Daten nicht an Dritte weitergeben
+ Mehrere Abteilungen, Teams, MitarbeiterInnen können parallel verwaltet werden
+ Intelligente Nachrichtentypenwahl
+ deutsches Unternehmen, deutsche Server
+ keine Nutzerauswertung
+ keine Weitergabe von Daten an Dritte
+ Kompatibilität (Smartphones, Tablets, Desktop,…)
+ automatische Synchronisation
- Kosten von 1,90€/NutzerIn/Monat in der Basic-Version und 4,90€/NutzerIn/Monat in der Pro-Version

Wickr

+ kostenlos
+ Daten werden schon vor dem Abschicken anonymisiert
+ alle Metadaten werden vor dem Versenden gelöscht
+ keine Angabe persönlicher Daten nötig, kein Auslesen persönlicher Daten
+ Ende-zu-Ende-Verschlüsselung
- Daten werden in den USA gespeichert
- Nachrichten, Anhänge usw. werden nicht automatisch gelöscht, lässt sich aber benutzerdefiniert festlegen

Briar

+ kommuniziert über das anonyme Tor-Netzwerk
+ NutzerInnen kommunizieren direkt miteinander, keine Datenbank steht dazwischen
+ bei der Nutzung fallen keine Metadaten an
+ keine zentralen Server
+ keinerlei persönliche Daten notwendig
+ kann auch ohne Internet funktionieren (Mesh-Networking)
+ Open Source
- alltägliche Nutzung ist wenig komfortabel
- nur für Android verfügbar
- keine Telefonie
- Kommunikation nur, wenn beide PartnerInnen online sind
- keine Backup-Funktion

Neue Kommunikationspartner können sich untereinander per Gerät-zu-Gerät kontakt bekanntmachen, sie müssen also zur gleichen Zeit am gleichen Ort sein. Briar wird z.B. von AktivistInnen und JournalistInnen verwendet.

Kontalk

+ ist ein unabhängiges Unternehmen, wird von Freiwilligen betrieben
+ kein Interesse an der Auswertung von NutzerInnendaten

+ offener Quellcode
+ alle Nachrichten sind immer verschlüsselt
+ Auf andere Kontakte wird nur via Hashes zugegriffen
+ keine Metadaten
+ jeder kann mitarbeiten
- sehr kleiner NutzerInnenkreis
- Projektfortschritt abhängig von Freiwilligenarbeit
- keine Audio- und Videotelefonate

Social Media

Diaspora

+ Datenschutz wird sehr hochgehalten
+ werbefrei
+ Open-Source-Projekt
+ dezentraler Aufbau der Plattform: Daten werden bei einzelnen Anbietern gespeichert
+ Schnittstellen mit anderen Social Media (Facebook und Twitter), sodass Nachrichten auch auf etablierten Social Networks veröffentlicht werden können
- technisches Know-How notwendig, um persönlichen Server einzurichten
- nur 50 000 NutzerInnen, d.h. keine hohe Reichweite
- keine App vorhanden

Alles in allem wird hier zwar auf verschiedenen Seiten die Grundphilosophie gut bewertet, allerdings ist die Nutzung höchstwahrscheinlich als eher mühsam anzusehen bzw. setzt diese einiges an technischem Know-how voraus.

NextDoor

+ Daten werden nicht an Dritte weitergegeben
- funktioniert nur lokal (also Nachbarschaft)
- amerikanische Server

Ist ein privates soziales Netzwerk für Kommunikation und Vernetzung innerhalb einer bestimmten Nachbarschaft. Dabei soll es darum gehen, das nachbarschaftliche Leben zu organisieren, gemeinsam Events zu planen und gegenseitige Hilfe zu fördern. (Diese Art von Social Media fällt eher unter „alternativ“ als unter „sicher“)

Wenn man z.B. wegen Umzug aus der Nachbarschaft ausscheidet, gehen die Kontakte verloren

nebenan.de

+ Server in Deutschland, TÜV-geprüft
+ Daten nur für Mitglieder der gleichen Nachbarschaft sichtbar
- enthält Werbung
- wird erst ab 50 Personen/Nachbarschaft aktiviert

Ist die deutsche Alternative für NextDoor. Mitglied kann man nur in der eigenen Nachbarschaft sein (die Zugehörigkeit zur Nachbarschaft muss nachgewiesen werden)

FragNebenan (Österreichische Nachbarschafts-plattform)

+ NutzerInnenschaft von 55.000 Personen
+ genaue Adresse ist nicht sichtbar

Vernetzungsplattform für Nachbarschaft, richtet sich v.a. an den urbanen Raum

https://fragnebenan.com/Datenschutz --> österreichische bzw. EU Datenschutzbestimmungen

Vero

+ Werbefrei (derz. noch)
+ keine Algorithmen, dh. es wird nicht angezeigt, was interessieren KÖNNTE, sondern das, was die Leute, denen man folgt, posten
+ sammelt keine Daten
- unklare Abo-Regelungen
- Direktverkaufsmöglichkeiten für Unternehmen auf der Plattform (soll in Zukunft möglich sein)
- Werbung durch Influencer

movim

+ Open Source-Software
+ dezentral, über mehrere Server verteilt
+ anonyme Anmeldung auf Pods
+ Chat Clients + Android App
+ Arbeitet mit XMPP – einem offenen, standardisiertem Instant Messanging Protokoll.
- eher kleine NutzerInnenschaft

„dezentral über mehrere Server verteilt“ bedeutet: Die NutzerInnen sind nicht an einen einzelnen Betreiber gebunden, d.h. sie können zu einem anderen wechseln, ohne aber das soziale Netzwerk selbst zu wechseln.

tellz.me App

+ keine Werbung
+ kein Datenverkauf
+ EU-DSGV
+ NutzerInnen können nur mit Einverständnis hinzugefügt werden und bestimmen, welche Information sichtbar ist.
- erweiterte Funktionen kosten etwas

tellz.me ist eine Mischung aus Messenger App und Social Network. Die App funktioniert mit Hilfe von „Channel Messaging“ und kann damit als Art „persönlicher Nachrichtensender“ verwendet werden. Man kann einen Channel erstellen, alles Mögliche teilen und dann Admin-, Schreib- und/oder Leserechte vergeben.

Wie funktioniert Channel Messaging? http://www.entdecke.tellz.me/channelmessaging.html

Ello

+ keine Datensammlung
+ unkommerziell
+ keine Klarnamenpflicht
+ keine Algorithmen
+ hohe Transparenz (welche Daten werden aufgezeichnet, welche z.B. an Google weitergeleitet und warum)
+ einfache Opt-Out Möglichkeiten für Datenschutzfragen

- plant die Beteiligung an Einnahmen von NutzerInnen, die über das Netzwerk Verkäufe tätigen.
- ist sehr einfach gehalten und hat noch weniger Funktionen als andere Plattformen

Credo: „Du bist kein Produkt“, hat es nicht in den Mainstream geschafft und positioniert sich jetzt als „Netzwerk für die kreative Klasse“ d.h. ist eine Fotoplattform für KünstlerInnen geworden

friendica

+ dezentralisierte Architektur
+ Möglichkeiten zur Verzahnung mit anderen Profilen (Facebook,…)
+ Daten und hochgeladene Materialien können nach gewisser Zeit gelöscht werden bzw. löschen sich selbst
+ volle Verfügung über die eigenen Daten
+ man kann sich aussuchen, auf welchem Server man die Daten speichert, kann auch eigenen Server installieren.
+ open source
+ kommuniziert mit: Diaspora, GNU Social, Pump.io, Mastodon und Pleroma.
+ wird von Freiwilligen entwickelt – keine Werbung, keine finanziellen Interessen

Hubzilla

+ Open Source-Software
+ dezentral, über mehrere Server verteilt
+ vom Funktionsumfang mit Facebook vergleichbar
+ man installiert eine Hubzilla Software und kann diese auf jedem beliebigen Knoten (Hub) installieren und betreiben.
+ völlige Datensouveränität
+ sichere Kommunikationskanäle
- es existieren keine Apps für Smartphone oder Tablet
- technisch anspruchsvoll

Mastodon

+ Open Source-Software
+ dezentral, über mehrere Server verteilt
+ kompatibel zu GNU Social
+ Wird durch Spenden finanziert, es steht kein finanzielles Interesse dahinter.
+ bietet effektive Anti-Missbrauchs-Werkzeuge
+ auch für Organisationen nutzbar
+ strikter Schutz gegen Belästigung und andere Inhalte wie Hetze
+ umfangreiche Moderation (bei unangebrachten Inhalten)

Ist eigentlich ein Microblogging-Dienst (500 Zeichen erlaubt)

GNU social

+ Open Source-Software
+ dezentral, über mehrere Server verteilt

GNU Social ist Teil der selben Foundation (Fediverse) wie Mastodon

Suchmaschinen

DuckDuckGo

+ sammelt keine persönlichen Informationen über die NutzerInnen
+ keine Speicherung von IP-Adressen
+ verwendet kaum Cookies

+ gute Ergebnisse
+ iOS und Android App
- Server in den USA

ixquick/Startpage

+ keine Speicherung der NutzerInnendaten
+ anonymes Öffnen von Websites
+ Verschleierung von IP Adressen
+ arbeitet mit anonymisierten Google-Suchergebnissen
+ Europäisches Datenschutz-Gütesiegel
+ Startseite verwendet standardmäßig eine sichere SSL Verbindung
+ es gibt Apps für iOS und Android
+ in den Einstellungen kann ausgewählt werden, ob ein amerikanischer oder europäischer Server verwendet werden soll

MetaGer

+ Server in Deutschland
+ Beim Besuch einer Website kann man sich hinter einem Proxy Server „verstecken“
+ es wird nichts getracked und gespeichert
+ Suchmaschine bietet einen Tor-Zugang
+ Android App
+ MetaGer2: sortiert die Suchergebnisse und eliminiert z.B. gefälschte Seiten

Meta-Suchmaschine, entwickelt an der Uni Hannover

Qwant

+ es wird jeweils ein Cookie für die entsprechende Sitzung gesetzt und nach Verlassen der Seite sofort gelöscht (eine permanente Browserdatei wird nicht angelegt).
+ keine Speicherung von NutzerInnendaten bzw. Informationen zum Nutzverhalten
+ keine Aufzeichnung von IP Adressen
+ Alle Suchergebnisse sind für alle gleich. Möchte man personalisierte Suchergebnisse, kann man ein Profil anlegen. Diese Daten werden ausschließlich auf EU Servern gespeichert.

Besonderer Fokus auf Sicherheit, Privatsphäre und kein Tracking, ist ein französisches Unternehmen.

Unbubble

+ hoher Datenschutz
+ neutrale Ergebnisse (möglichst frei von subjektiven Wertvorstellungen)
+ Schutz gegen Überwachung und Manipulation
+ deutsche Server
+ Suchergebnisse werden mit Datenherkunft angezeigt
+ Meta-Suchmaschine

Mehr **Tipps und Infos** zur Digitalen Professionalisierung in der Erwachsenenbildung finden Sie unter https://erwachsenenbildung.at/digiprof/.

Medieninhaber/Herausgeber: Bundesministerium für Bildung, Wissenschaft und Forschung | Redaktion: Verein CONEDU