RATGEBER

Sichere Kommunikation in der Kinder- und Jugendarbeit



BDKJ
Bund der Deutschen Katholischen Jugend
Diözese Rottenburg-Stuttgart

IMPRESSUM

Herausgeber:
BDKJ-Diözesanverband Rottenburg-Stuttgart
Antoniusstraße 3
73249 Wernau

Redaktion:
Susanne Grimbacher, Lukas Jaeckle, Pedro Martins, Michael Medla
(Mitglieder der AG Digitalisierung)

ViSdP:
Michael Medla (Diözesanleitung BDKJ / BJA)

Layout und Satz:
Marcel Krämer (Stabstelle Öffentlichkeitsarbeit)

Disclaimer:
Alle in unserem Ratgeber enthaltenen Angaben und Informationen wurden sorgfältig recherchiert und geprüft. Für Richtigkeit, Vollständigkeit und Aktualität können wir keine Haftung übernehmen.

1. Ausgabe - Oktober 2021

VORWORT

Dieser Ratgeber wurde von der Arbeitsgruppe „Digitalisierung“ des BDKJ Rottenburg-Stuttgart im Auftrag der Diözesanversammlung erstellt. Der Ratgeber gibt Empfehlungen für sichere Tools zur Kommunikation und Kollaboration, zum anderen erklärt er, welche Kriterien hinsichtlich der Aspekte Datenschutz und Security wichtig sind, sodass sich jede*r selbst informieren kann, ob er*sie ein Tool einsetzen möchte.

ERLÄUTERUNG

★★★★★ Bewertung (1 Stern „schlecht“, 5 Sterne „sehr gut“)



Logo und Land des Firmen- bzw. Betreiber*innensitzes



Datensicherheit



Datenschutzerklärung



Besonderheiten

INHALTSVERZEICHNIS

Vorwort 3

Empfehlungen auf einen Blick 5

- Messenger 6
- Kollaborationstools 9
- Videokonferenztools 12

Glossar 15

Datenschutz in der Jugendarbeit 18

- Welches Datenschutzgesetz gilt? 19
- Grundlagenwissen zur DSGVO 19
- Ein konkretes Beispiel 20
- Was sind eigentlich Daten? 22
- Folgen und Grenzen für die Praxis 23
- Datenschutz - wieso eigentlich? 23
- Bewertungskriterien 24
- Zusammenhang zwischen Kategorien und der Bewertung 26

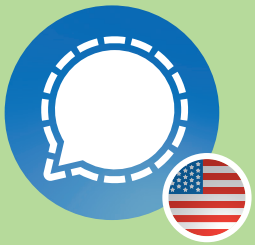
Empfehlungen ausführlich erklärt 27

- Messenger 28
- Kollaborationstools 35
- Videokonferenzdienste 40

Verweise 46

EMPFEHLUNGEN AUF EINEN BLICK





SIGNAL

★ ★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

Signal nutzt für alle Nachrichten eine Ende-zu-Ende Verschlüsselung. Signal hat zudem quasi keinen Zugriff auf Metadaten.

Die Datenschutzerklärung von Signal ist vorbildlich.

Signal ermöglicht einen Desktop-Client. Gruppenanrufe sind mit max. 15 Personen möglich.



THREEMA

★ ★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

Threema nutzt für alle Nachrichten eine Ende-zu-Ende Verschlüsselung. Threema hat zudem quasi keinen Zugriff auf Metadaten.

Die Datenschutzerklärung von Threema ist vorbildlich.

Threema kennzeichnet Kontakte mit einer „Verifizierungsstufe“, die empfiehlt, welche Kontakte aus dem Adressbuch kontaktiert werden sollten.

WHATSAPP

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

WhatsApp nutzt für alle Nachrichten eine Ende-zu-Ende Verschlüsselung. Jedoch nutzt WhatsApp die Metadaten seiner Nutzer*innen.

Die Datenschutzerklärung von WhatsApp erklärt, dass Daten mit anderen Facebook-Produkten geteilt werden.

WhatsApp ermöglicht die Erstellung von Stories.
Darüber hinaus bietet WhatsApp die Möglichkeit, Nachrichten durch Moderationen auf ihre Richtigkeit hin überprüfen zu lassen. So können Fake-News gemeldet werden.

TELEGRAM

★ ★

Geeignet für Daten der **Datenschutzklasse 1**

Telegram nutzt keine Ende-zu-Ende Verschlüsselung. Telegram hat Zugriff auf die Metadaten der Nutzer*innen.

Die Datenschutzerklärung von Telegram ist intransparent formuliert und ermöglicht die Nutzung von Daten durch Dritte (z.B. durch Bots).

FACEBOOK MESSINGER & INSTAGRAM-DIRECT

Geeignet für Daten der **Datenschutzklasse 0**

Beide Messenger bieten keine Ende-zu-Ende Verschlüsselung an. Beide Dienste haben keine Maßnahmen etabliert, um Metadaten zu reduzieren.

Beide Dienste nutzen alle anfallenden Daten für zielgerichtete Werbeprofile.

Instagram und Facebook ermöglichen das Auffinden von Kontakten ohne Telefonnummer, E-Mail oder Threema-ID.

SNAPCHAT

Geeignet für Daten der **Datenschutzklasse 0**

Eine Bewertung dieses Aspektes ist aufgrund von Intransparenz nicht möglich. Entsprechend der Datenschutzerklärung von Snapchat werden viele Metadaten gesammelt.

Die Datenschutzerklärung weist darauf hin, dass Snapchat Daten mit Dritten teilt.

Snapchat weist darauf hin, dass mit Snapchat geteilte Nachrichten nach einer gewissen Zeit zwar automatisch gelöscht werden, Nachrichten jedoch digital kopierbar sind.



ELEMENT

basierend auf Matrix

★ ★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**



Element bietet eine optionale Ende-zu-Ende Verschlüsselung an. Element erfasst nur benötigte Metadaten.



Element stellt eine gut verständliche und transparente Datenschutzerklärung aus, die angemessen ist.



Element kann selbst gehostet werden.



ROCKET.CHAT

★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**



Rocket.Chat bietet eine Ende-zu-Ende Verschlüsselung für Nachrichten an. Rocket.Chat hat keine Maßnahmen etabliert, um Metadaten zu reduzieren.



Die Datenschutzerklärung von Rocket.Chat ist vorbildlich.



Rocket.Chat kann selbst gehostet werden.



MICROSOFT TEAMS

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**



Microsoft Teams bietet keine Ende-zu-Ende Verschlüsselung an. Teams hat keine Maßnahmen etabliert, um Metadaten zu reduzieren.



Die Datenschutzerklärung von Microsoft Teams ist angemessen.



Microsoft Teams ist seit Oktober 2021 fester Bestandteil von Windows 11 & der Microsoft Office-Suite.



SLACK

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**



Slack bietet keine Ende-zu-Ende Verschlüsselung an. Slack hat keine Maßnahmen etabliert, um Metadaten zu reduzieren.



Die Datenschutzerklärung von Slack ist angemessen.



An Slack Calls können max. 15 Teilnehmer teilnehmen. Eine Integration von Zoom ist in Slack möglich um Konferenzen mit mehr Nutzer*innen zu ermöglichen.



DISCORD

★ ★

Geeignet für Daten der **Datenschutzklasse 1**

Discord bietet keine Ende-zu-Ende Verschlüsselung an. Discord hat bewusst keine Maßnahmen etabliert, um Metadaten zu reduzieren.

Die Datenschutzerklärung von Discord ist weitgehend intransparent.

Discord basiert auf der Idee, dass Nutzer*innen selbst Communities erstellen können, die mitunter auch viele 100.000 Nutzer*innen groß sind.
Die Einbindung von Facebook oder Twitter in das Discord Konto ist möglich.



JITSI MEET

★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

Jitsi Meet bietet eine optionale Ende-zu-Ende Verschlüsselung an. Jitsi Meet erhebt nur wenige Metadaten.

Die Datenschutzerklärung von Jitsi Meet ist vorbildlich.

Jitsi Meet kann selbst gehostet werden.



BIG BLUE BUTTON (BDKJ)

★ ★

Geeignet für Daten der **Datenschutzklasse 1**

BBB bietet keine Ende-zu-Ende Verschlüsselung an. Eine BBB Anwendung kann sehr viele Metadaten über Sitzungen erfassen.

Der Betreiber der BBB-Instanz - IT-Abteilung des BDKJ/BJA – stellt zurzeit keine Datenschutzerklärung aus.

BBB ist durch den BDKJ/BJA selbst gehostet.



ZOOM

★ ★

Geeignet für Daten der **Datenschutzklasse 1**



Zoom bietet eine optionale Ende-zu-Ende Verschlüsselung an. Zoom hat keine Maßnahmen etabliert, um Metadaten zu reduzieren.



Die Datenschutzerklärung von Zoom lässt die genaue Nutzung der Daten offen.



Zoom läuft erfahrungsgemäß sehr stabil.



ZOOM ON-PREMISE (WGKD)

★ ★

Geeignet für Daten der **Datenschutzklasse 1**



Zoom On-Premise bietet eine optionale Ende-zu-Ende Verschlüsselung an. Zoom On-Premise hat keine Maßnahmen etabliert, um Metadaten zu reduzieren.



Die Datenverarbeitung bzgl. der Besprechungsinhalte kann von der WGKD vertraglich mit dem Hoster geregelt werden. Die vertragliche Vereinbarung lag den Erstellern des Ratgebers aber nicht vor.

WEBEX

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**

WebEx bietet eine optionale Ende-zu-Ende Verschlüsselung an. WebEx erhebt Metadaten zweckgebunden.

Die Datenschutzerklärung von WebEx ist transparent, welche Daten sie erheben und warum sie dies tun. Allerdings verarbeitet WebEx viele personenbezogene Daten.

WEBEX (DRS)

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**

Siehe WebEx.

Siehe WebEx.

Es können eigentlich keine Unterschiede zur normalen Variante ausgemacht werden. Sehr wahrscheinlich dürfte vertraglich die Speicherung der Daten in Frankfurt vereinbart worden sein.

GLOSSAR



Datenresidenz

Unter Datenresidenz wird meist die Speicherung von ruhenden Daten verstanden. Manche Hersteller ermöglichen Nutzer*innen den Standort der Server für die Speicherung von ruhenden Daten festzulegen. Datenresidenz wird zunehmend von Unternehmen eingefordert, damit die Daten ihrer Nutzer*innen prinzipiell entsprechend der Unternehmensrichtlinien und regulatorischer Vorgaben abgelegt werden.

DSGVO

Die Datenschutzgrundverordnung, bzw. im englischen General Data Privacy Regulation, wird in dem Kapitel „Datenschutz in der Jugendarbeit“ näher beschrieben.

Ende-zu-Ende-Verschlüsselung

Die Ende-zu-Ende Verschlüsselung, bzw. im englischen end-to-end-encryption, wird in dem Kapitel „Bewertungskriterien“ näher beschrieben.

IP-Adresse

Eine IP-Adresse ist eine technische Adresse. IP steht dabei für „Internetprotokoll“. Vergleichbar ist die Adresse mit einer Anschrift, die wir für Briefe und Pakete angeben müssen. Jedes mit dem Internet verbundene Geräte erhält eine solche IP-Adresse zugewiesen, wodurch Nachrichten adressierbar werden. Obwohl die Adresse technischer Art ist, ist mindestens dem Kommunikationsanbieter bekannt, welche Adresse zu welchem Vertragsinhaber gehört. Daher ist die IP-Adresse personenbeziehbar.

Metadaten

Metadaten sind zusätzliche Daten, die bei jeder Kommunikation anfallen. Neben dem Gesprächsinhalt gibt es weitere Informationen, z.B. wer mit wem wie lange spricht. Im digitalen Bereich sind Metadaten sehr aufschlussreich, da z. B. die Größe einer Nachricht u.a. verraten kann, ob eine Textnachricht, eine Sprachnachricht, ein Bild oder ein Video geteilt wird. Durch die digitalen Anschriften (IP-Adressen, Telefonnummern, …) kann zudem abgeleitet werden, wo sich eine Person ungefähr aufhält. Auch wie oft jemand mit jemand anderem kommuniziert, usw. wird schon aus Metadaten ersichtlich.

Ruhende Daten

Ruhende Daten sind Daten, die auf einem ausgeschalteten Endgerät liegen, z.B. Bilder auf einem ausgeschalteten Handy oder Laptop. Sobald ein Gerät an ist, kann auf die Daten zugegriffen werden, sodass diese nicht mehr „ruhend“ sind.

Social-Engineering

Beim Social Engineering versucht ein*e Angreifer*in zunächst ein paar Informationen über eine Person zu sammeln. Diese Daten werden genutzt, um das Vertrauen des Opfers zu gewinnen, indem er*sie die erlangten Informationen in ein Gespräch/eine Anfrage einbaut. Dadurch wirkt ein*e Angreifer*in kompetent und erweckt den Eindruck, dass er*sie weitere Informationen bekommen darf. Dies könnten z. B. Zugangsdaten wie Passwörter sein. Oft versuchen Angreifer*innen auch ein Opfer zum Öffnen von Anhängen oder zum Anklicken von Links zu verleiten. Dadurch können sie sich Zugang zu einem Endgerät des Opfers verschaffen.

Transportverschlüsselung

Die Transportverschlüsselung, bzw. im englischen encryption-at-transit, wird in dem Kapitel „Bewertungskriterien“ näher beschrieben.

Verarbeitung

Nach Art. 4 der DSGVO bezeichnet „Verarbeitung“ alles, was mit personenbezogenen Daten geschehen kann, z.B. „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Verschlüsselung ruhender Daten

Die Verschlüsselung ruhender Daten, bzw. im englischen encryption-at-rest, wird in dem Kapitel „Bewertungskriterien“ näher beschrieben.

DATENSCHUTZ IN DER JUGENDARBEIT



Welches Datenschutzgesetz gilt?

Der BDKJ und seine Mitgliedsverbände fallen in den Gültigkeitsbereich des KDG („Gesetz über den Datenschutz in der katholischen Kirche“ [2]), welches seinerseits auf der europäischen DSGVO („Datenschutz-Grundverordnung“ [3]) aufbaut[1]. In der DSGVO ist der Kirche die Möglichkeit eingeräumt worden, für ihre Datenschutzanliegen selbst eine Regelung zu finden[2]. Allerdings darf die Kirche dies nur unter der Auflage, dass das KDG die Regelungen der europäischen Verordnung nicht unterschreitet. Weil das KDG mit der DSGVO vergleichbar ist, haben wir uns für den vorliegenden Ratgeber an den Regelungen der DSGVO orientiert, um den Ratgeber auch uneingeschränkt über unsere verbandliche Jugendarbeit hinaus nutzen zu können.

Im BDKJ gilt das kirchliche Datenschutzgesetz. Das ist vergleichbar mit dem staatlichen Datenschutzgesetz.

Einfach gesagt!

Grundlagenwissen zur DSGVO

Die DSGVO dient dem Schutz der persönlichen Daten. Daher verbietet sie zunächst grundsätzlich die ungeregelte Verarbeitung aller Daten. Stattdessen formuliert sie in Art. 6 Regeln, nach welchen Bedingungen Daten verarbeitet werden dürfen. Eine Verarbeitung ist u. a. nur durch „Einwilligung“, „Vertrag“, „gesetzliche Verpflichtung“ und ein „berechtigtes Interesse“ erlaubt. Für uns in der Jugendverbandsarbeit ist insbesondere die Möglichkeit der „Einwilligung“ interessant. Sie wird beispielsweise immer dann angewandt, wenn durch Formulare die Einwilligung zur Veröffentlichung von Fotos eingeholt werden.

Das Datenschutzgesetz erklärt, wie mit Daten umgegangen werden muss. Wer Daten verarbeitet, braucht die Zustimmung der betroffenen Person.

Einfach gesagt!

Des Weiteren regelt die DSGVO die „Rechte der Betroffenen“. D.h. jede*r von uns hat immer und jederzeit u. a. die folgenden Rechte in Bezug auf seine*ihre Daten:

- Art. 15 - Das Recht auf Auskunft
  Jede*r hat das Recht zu verstehen, wozu die eigenen Daten genutzt werden.
- Art. 16 - Das Recht auf Berichtigung
  Jede*r hat das Recht falsche Daten unverzüglich korrigieren zu lassen.
- Art. 17 - Das Recht auf Löschung
  Jede*r hat das Recht eigene Daten löschen zu lassen.
  Anmerkung: Der Aufforderung muss zwar unverzüglich nachgekommen werden, in der Praxis darf die Löschung einen für die löschende Person zumutbarem Zeitrahmen benötigen.
- Art. 18 - Das Recht auf Einschränkung der Verarbeitung
  Jede*r hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen

1 Zu den Kriterien, wann Verbände als sonstige kirchliche Rechtsträger gelten: https://www.dbk.de/themen/kirche-staat-und-recht/datenschutz-faq
2 s. Artikel 91 DSGVO.

- Art. 21 - Das Recht auf Widerspruch
  Jede*r hat das Recht Widerspruch gegen die weitere Verarbeitung einzulegen.

Ein konkretes Beispiel…

Die DSGVO schützt durch klare Regelungen „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ (Art. 1 DSGVO).
Um bei dem Beispiel der Einwilligung bzgl. der „Veröffentlichung von Bildern“ zu bleiben, bedeutet das Recht auf „Auskunft“, dass die betroffene Person für eine Einwilligung verständlich darüber informiert sein muss, wie ein Bild verarbeitet werden soll.
Die Frage in der praktischen Anwendung: Wann ist eine Auskunft verständlich genug? Ist eine Auskunft verständlich genug, wenn in einem Einwilligungsformular z. B. steht „Dein Bild wird zur Öffentlichkeitsarbeit unseres Verbandes auf Instagram gepostet“? Fragen die aufkommen könnten wären z. B. „Wer postet das Bild?“, „Wer kann das Bild dann einsehen?“, „Willigt die Person wissentlich ein, dass das Bild von anderen Nutzern digital kopiert und manipuliert werden kann?“[3] u.v.m.
Das Dilemma, sobald eine dieser Fragen für eine einwilligende Person nicht klar beantwortbar ist, kann die Einwilligung unwirksam sein. In der Folge hätte die „veröffentlichende Person“ gegen die DSGVO verstoßen.

Wenn beispielsweise Lisa ein Foto von Martin macht und dieses auf ihrem Instagram-Kanal posten möchte, braucht sie die Zustimmung von Martin. Dabei sollte Martin ganz genau wissen, was Lisa mit dem Foto machen möchte.

Einfach gesagt!

In der Praxis müssen aber nicht alle etwaige Fragen bis ins Kleinste beantwortet werden. Wichtig ist, dass wir uns der Notwendigkeit eines sorgsamen Umgangs mit den Daten bewusst sind. Das bedeutet, dass wir nur die Daten abfragen, die wir wirklich benötigen und dabei möglichst genau beschreiben, wofür wie sie benötigen. Erkennt die einwilligende Person die Datensparsamkeit und den Mehrwert, der durch die Einwilligung zur Nutzung der Daten entsteht, ist die Absicht hinter der DSGVO richtig umgesetzt.

In der täglichen Arbeit ist es wichtig, mit den Daten von anderen sorgsam umzugehen.

Einfach gesagt!

3 Ohne eine Einwilligung von der Person untersagt die DSGVO dies zwar, aber technisch ist dies möglich.2 s. Artikel 91 DSGVO.

Was sind eigentlich Daten?

Daten sind im Grunde jede Art von Informationen. Dabei werden diese Kategorien von Daten unterschieden:

- Daten, die nichts mit Personen zu tun haben (z. B. Anträge)
- personenbeziehbare Daten (z. B. in einer Gruppe sind Vegetarier*innen)
- personenbezogene Daten (z. B. Name eine*r Teilnehmer*in)

In der Jugendarbeit verarbeiten wir alle Arten von Daten. Da nicht alle Arten von Daten gleichermaßen geschützt werden müssen, werden sie in verschiedene Datenschutzklassen eingeordnet. Dabei ist 0 die niedrigste Klasse und 3 die höchste.

- Datenschutzklasse 0
  Weder personenbeziehbare noch personenbezogene Daten
- Datenschutzklasse 1
  Personenbeziehbare Daten – d. h. es darf kein direkter Bezug zu einer Person vorliegen. Jedoch ist es möglich, einen indirekten Bezug - auch über externe Daten – zu einer Person herzustellen.
- Datenschutzklasse 2
  Personenbezogene Daten, d. h. direkter Bezug zu einer Person
- Datenschutzklasse 3
  Personenbezogene oder -beziehbare und unter besonderem Schutz stehende Daten wie rassische oder ethische Herkunft; politische Meinung; religiöse oder weltanschauliche Überzeugung[4]; Gewerkschaftszugehörigkeit; Genetische Daten; Biometrische Daten; Gesundheitsdaten; Sexualleben und sexuelle Orientierung

Daten sind Informationen. Es gibt unterschiedliche Arten von Daten. Diese verdienen einen unterschiedlichen Schutz. Dein Name und deine Handynummer müssen besser geschützt werden als die Vorbereitung für eine Gruppenstunde.

Einfach gesagt!

Beispiele für die Jugendverbandsarbeit

Nachfolgend sind exemplarisch Daten aufgeführt und zugeordnet, die wir in unserer alltäglichen Jugendverbandsarbeit verarbeiten. Exemplarisch meint hier, dass die konkrete Zuordnung im Einzelfall festgelegt werden muss und daher abweichen kann. Dennoch soll diese Liste einen ersten Anhaltspunkt geben.

Datenschutzklasse 0: Nicht personenbeziehbare /-bezogene Daten:

- Anträge für die Kreisjugendringe, Dekanatsräte, Konferenzen, DiV, …
- Werbung und Organisation von Aktionen, Freizeiten, Gruppenstunden, Demonstrationen, Podiumsdiskussionen, …

4 Hier geht es um die Überzeugung. D.h. wenn wir in der Jugendverbandsarbeit erfassen würden, wie ein*e Jugendliche*r seinen*ihren Glauben auslegt, dann würde dies in die Datenschutzkategorie 3 fallen. Allein, dass wir als katholische Jugendverbandsarbeit aktiv sind, bedeutet allerdings noch nicht, dass alle unsere Teilnehmendenlisten Ausdruck einer Weltanschauung und damit nach Kategorie 3 zu behandeln sind. Nur, weil jemand bei uns mitmacht, heißt das nicht, dass er*sie dieser Weltanschauung per se nahesteht.

Datenschutzklasse 1: Personenbeziehbare Daten:

- Geburtsdaten / Alter von Teilnehmenden in Förderanträgen
- Anzahl von Vegetarier*innen / Veganer*innen auf einer Freizeit
- Sammlung von Threema IDs

Datenschutzklasse 2: Personenbezogene Daten:

- Teilnehmer*innenlisten, Telefonbücher und ähnliches wenn Daten wie Namen, Telefonnummern, Mailadressen, Anschriften, … enthalten sind
- Fotos & Videos von Veranstaltungen auf denen Personen erkennbar sind

Datenschutzklasse 3: Daten unter besonderem Schutz:

- Allergien, Medikamente, Krankheiten
- Bewerbungsunterlagen

Folgen und Grenzen für die Praxis

Aus der Einteilung in Datenschutzklassen ergeben sich Konsequenzen für unsere Arbeit. Umso höher die Datenschutzklasse, desto sorgfältiger muss mit den Daten umgegangen werden. Ein Beispiel:
Eine kurze Nachricht wie „Sepp kann nicht kommen, der hat mal wieder die Grippe“ in einem Chat ist problematisch. Denn dabei werden Gesundheitsdaten der allerhöchsten Datenschutzkategorie mal eben schnell geteilt. Prinzipiell könnte die betroffene Person nun mit Rechtsmitteln gegen den*die Verfasser*in der Nachricht vorgehen. Die Nachricht dürfte nur lauten: „Sepp kann nicht kommen.“

In der katholischen Kinder- und Jugendverbandsarbeit beschäftigen wir uns häufig mit unseren religiösen und politischen Überzeugungen. Diese gehören der Datenschutzklasse 3 an und sind besonders schützenswert. Deshalb sollten wir Daten nur zweckgebunden erheben, unsere Kommunikationsmittel achtsam auswählen und uns und andere gut über den Datenschutz informieren.

Umso persönlicher Daten sind, desto besser müssen sie geschützt werden. Das gilt auch für uns im BDKJ. Wir überlegen genau, welche Daten wir brauchen und wie wir mit ihnen umgehen.

Einfach gesagt!

Datenschutz – wieso eigentlich?

Vermutlich kennt jede*r von uns die extremen Standpunkte in der Diskussion um den Datenschutz. Solche Standpunkte sind u. a. „ich habe ja nix zu verbergen“, „meine Daten interessieren ja eh niemand“ oder „Regierungsbehörden wie die NSA und die großen Unternehmen haben doch sowieso Zugriff auf alles“. Die nachfolgende Betrachtung soll diese Standpunkte hinterfragen und für einen guten Umgang mit Daten sensibilisieren, denn bei näherer Betrachtung dieser Statements

wird ersichtlich, dass sich die Frage um den Datenschutz auch darum dreht, vor wem wir unsere Daten schützen. Nachfolgend sind ein paar potenzielle Interessent*innen an personenbezogenen Daten aufgeführt.

Wenn man verstehen will, weshalb Datenschutz wichtig ist, muss man erst verstehen, w

Einfach gesagt!

Regierungsbehörden

- Durch Mitlesen von Nachrichten wird es einer Regierungsbehörde mit Fokus auf der inneren Sicherheit möglich, frühzeitig die Vorbereitung von Straftaten mitzubekommen und die Tat zu vereiteln, noch bevor sie ausgeführt wird [4] [5].
- Durch Mitlesen von Nachrichten wird es einer Regierungsbehörde möglich, u. a. Gesinnungen von Nutzer*innen zu erkennen und die Personen entsprechend zu verfolgen[5] [6].

Dienstanbieter

- Durch Mitlesen von Nachrichten wird es einem Dienstanbieter möglich, detaillierte Nutzer*-innenprofile einschließlich der Vorlieben zu erstellen. Bei werbetreibenden Unternehmen werden diese für möglichst akkurate Werbungen monetarisiert [7].
- Bei Unternehmen, die Mitarbeitenden Zugriff auf solch möglichweise intimen Daten ermöglichen, können solche Daten ggf. zur Erpressung genutzt werden[6] [8].
- Durch Mitlesen der Metadaten wird es einem Dienstanbieter möglich, nachzuvollziehen wer mit wem häufig/selten kommuniziert. Dies ist vollkommen
- ausreichend, um soziale Cluster zu identifizieren. Z. B. wird Werbung, die einer Person gut gefallen hat, dann für das gesamte Cluster aus vermutlich gleichen Interessen angezeigt [9].

Böswillige Freund*innen, Kolleg*innen, …

- In unserer Jugendverbandsarbeit setzen wir uns bereits gegen (Cyber-)Mobbing [10] ein. Cybermobbing hat leider viele Ausprägungen, wie z. B. wenn Täter*innen aus dem direkten sozialen Umfeld ein Handy stehlen und mit dem zuvor ausspioniertem Speercode falsche Nachrichten unter der Identität des Opfers versenden [11].

Böswillige Dritte

- Hauptfokus von Dritten ist die Übernahme von Accounts, was dadurch, dass Zugangsdaten meist einfach zu erraten oder durch sogenanntes Social-Engineering ermittelbar sind, nicht schwerfällt. Mit Zugriff auf die eigentlichen Daten können Angreifer*innen die betroffene Person meist erpressen, sehr realistische Fake-Profile auf anderen Diensten erstellen und durch den Verkauf von Nutzer*innendaten ihre Aktionen unmittelbar monetarisieren [12].

Diese Liste ist zwar nicht vollständig, dient aber einer ersten Sensibilisierung für die Bedeutung des Datenschutzes. Zentral ist der Schutz der eigenen Daten durch starke Zugangsdaten (wie lange und schwer zu erratenden Passwörtern und Zwei-Faktor Authentifizierung) und gut aufgestellte Dienstanbieter bzw. aktuelle Softwareinstallationen. Außerdem ist Vorsicht bei verdächtigen Mails

5 Dies ist in den meisten Europäischen Ländern kein Problem. Kniffeliger wird's, wenn die Kommunikation in anderen Ländern dieser Welt geführt wird, in denen die Meinungsfreiheit weit weniger geschützt ist.

6 Dies gilt insbesondere bei selbst gehosteten Anwendungen, bei denen u.U. die Mitarbeitenden des Dienstanbieters sogar die Nutzer direkt kennt.

mit Anhängen geboten. Das Bundesamt für Sicherheit in der Informationstechnik veröffentlicht regelmäßig gute Ratgeber für Unternehmen und Behörden (z. B. [13]), die aber auch uneingeschränkt im privaten Umfeld anwendbar sind.

Wer deine Daten hat, kann sie gegen dich verwenden. Deshalb solltest Du deine Daten schützen. Das kannst du durch schwierige Passwörter tun.

Einfach gesagt!

Bewertungskriterien

Kategorie 1: Technischer Datenschutz

Um zu verstehen, wie Daten sicher verarbeitet werden können, sind folgende technische Grundlagen hilfreich:

Erstens sollten moderne und von Expert*innen empfohlene Verschlüsselungsverfahren bevorzugt werden. Unter der „Verschlüsselung“ wird verstanden, dass alle (Sprach-)Nachrichten, (Video-) Anrufe, Bilder, etc., die über eine App versendet werden, nur von den beabsichtigten Personen gelesen werden können. Gute Empfehlungen geben hier besonders Behörden wie das „Bundesamt für Sicherheit in der Informationstechnik“ oder die „National Security Agency“. Wichtig ist dabei, dass nur wenige Verfahren mit entsprechenden Parametern als besonders sicher gelten und das jedes Verfahren in einem bestimmten Einsatzgebiet glänzt.

Ein kurzer Exkurs: Idealerweise wird die Kommunikation zwischen Geräten und einem Server mittels TLSv1.3 abgesichert (Transportverschlüsselung). Daten die auf einem Rechner, Smartphone oder auf einem Server liegen, sollten mit XTS-AES und einem langen, hardwareseitig gesicherten Schlüssel abgelegt sein (Verschlüsselung ruhender Daten). Neben diesen beiden, in der Infrastruktur umsetzbaren, Aspekten sollten die verschickten Nachrichten zusätzlich selbst verschlüsselt sein (Ende-zu-End). Bei Messengern gilt derzeit das „Signal“-Protokoll als das Beste. Wichtig ist dabei: Idealerweise werden alle drei Absicherungen genutzt. Denn erst durch eine Ende-zu-Ende Verschlüsselung hat der Anbieter eines Dienstes keine Möglichkeit, die Inhalte von Nachrichten einzusehen. Fehlt neben einer Ende-zu-Ende Verschlüsselung zusätzlich eines der anderen Verschlüsselungsverfahren, ist die Wahrscheinlichkeit sehr groß, dass Dritte Zugriff auf Nachrichten bekommen.

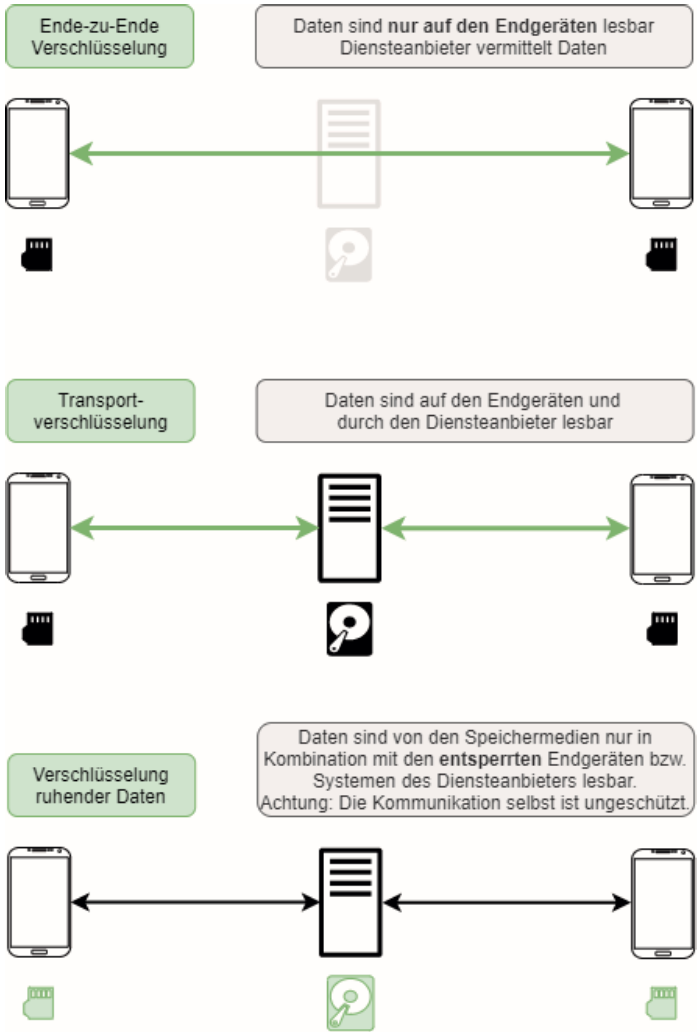
Zweitens bei jeder Kommunikation fallen zusätzliche Daten an. Diese werden Metadaten genannt und beinhalten Informationen wie z. B. wer mit wem gerade kommuniziert, wie groß die Nachricht ist (Bilder brauchen mehr Daten als ein paar Sätze), wie oft jemand mit jemand anderem kommuniziert, usw. Metadaten können daher sehr viel verraten, wie z. B.:

- haben eine Menge von Personen zurzeit die gleiche IP-Adresse, sitzen sie vermutlich im selben Haus. Ist dabei die IP-Adresse von einer Person nicht anders als sonst, sind wohl alle weiteren Personen bei dieser einen Person zu Besuch.
- Hat eine Person Werbung angeklickt und teilt diesen Link an eine andere Person, kennen sich

beide Personen und haben vermutlich ähnliche Interessen.

- Werden plötzlich sehr viele Nachrichten geteilt und ist es womöglich eine Nachricht mit einer ähnlichen Größe, handelt es sich wohl um eine brisante Nachricht (Kettenbriefe, …)

Hier lassen sich sehr viele Beispiele aufführen. Werbetreibende Unternehmen können schon durch solche Metadaten Gewinne erzielen. Die Vermeidung von Metadaten ist dabei alles andere als einfach. Technisch gesehen gibt es weltweit nur wenige Dienste[7], die hier versuchen nach dem Zero-Knowledge-Prinzip, Metadaten zu reduzieren oder unbrauchbar zu machen.



Ein kurzer Exkurs: Aufgrund dessen, dass Android ab Version 6.0 [14] und iOS ab Version 7.0 [15] grundsätzlich ab Werk die Partitionen verschlüsseln, ist vor allem die Verschlüsselung ruhender Daten bei vielen Endgeräten gewährleistet. Bei Laptops ist die Situation etwas unübersichtlicher. Grundsätzlich besteht auch hier mit z. B. Bitlocker (Bestandteil von Windows) die Möglichkeit die Daten effektiv zu verschlüsseln, aktiv ist die Option aber leider nicht unbedingt auf jedem Gerät. Dennoch wird die Verschlüsselung ruhender Daten in diesem Ratgeber aufgrund der verfügbaren Absicherung der Endgeräte nur auf der Dienstanbieterseite betrachtet.

Kategorie 2: Organisatorischer Datenschutz

Diese Kategorie wird dann interessant, wenn ein Anbieter keine Ende-zu-Ende Verschlüsselung umsetzt und zugleich die anfallenden Metadaten nicht reduziert. In diesen Situationen kommt es darauf an, wie viel Datenschutz ein Anbieter zusichert. Dieser Ratgeber berücksichtigt die Datenschutzerklärungen insofern, dass die höchste Datenschutzklasse auch bei einer fehlenden Ende-zu-Ende Verschlüsselung erreicht werden kann, wenn die Verarbeitung der Daten durch den Anbieter verhältnismäßig erfolgt. Zugleich führt eine unverhältnismäßige oder fehlende Datenschutzerklärung (und damit eine mögliche Weitergabe der Daten) zu einem Abzug.

7 Das TOR-Projekt ist eines davon, um die Kommunikation von Journalist*innen zu verschleiern.

Kategorie 3: Besonderheiten

Neben den technischen Aspekten und den Datenschutzregularien, die eine objektive Bewertung von Diensten ermöglichen, gibt es weitere subjektive Aspekte, die die Wahl eines Dienstes positiv/negativ beeinflussen können:

- Ist eine theoretische Überprüfbarkeit der Implementierung durch Open-Source gegeben oder werden idealerweise regelmäßig Audits des Quellcodes durchgeführt?
- Welches Geschäftsmodell ermöglicht den Betrieb eines Dienstes?
- Gibt es moderierende Funktionen für Nachrichten, wie die Begrenzung von Weiterleitungen, einen Fakten-Checker, etc.?
- Besondere Funktionen (Bildschirm teilen, Stories, …)

Zusammenhang zwischen Kategorien und der Bewertung

Die Bewertungen in diesem Ratgeber setzen sich wie folgt zusammen:

5 Sterne	Datenschutzklasse 3	Ende-zu-Ende Verschlüsselung Technische Reduktion von Metadaten
5 Sterne	Datenschutzklasse 3	Ende-zu-Ende Verschlüsselung Verhältnismäßige Datenschutzerklärung
4 Sterne	Datenschutzklasse 3	Optionale Ende-zu-Ende Verschlüsselung ohne nennenswerte Funktionseinschränkungen bzw. starke Transportverschlüsselung Verschlüsselung ruhender Daten Verhältnismäßige Datenschutzerklärung
3 Sterne	Datenschutzklasse 3	Ende-zu-Ende Verschlüsselung
3 Sterne	Datenschutzklasse 2	Starke Transportverschlüsselung Verschlüsselung ruhender Daten Verhältnismäßige Datenschutzerklärung
2 Sterne	Datenschutzklasse 1	Starke Transportverschlüsselung Verschlüsselung ruhender Daten
1 Stern	Datenschutzklasse 0	Fehlende Ende-zu-Ende Verschlüsselung und Transportverschlüsselung
1 Stern	Datenschutzklasse 0	Unverhältnismäßige oder fehlende Datenschutzerklärung

Damit deine Daten sicher sind, sollten sie verschlüsselt sein. Manche Anbieter können sogar mitlesen, was du schreibst, andere können nicht einmal einsehen, mit wem du schreibst. Desto weniger ein Anbieter weiß, desto besser. Bei den Bewertungen findest du die Verschlüsselung unter „Technischer Datenschutz“ beschrieben.
Bei „organisatorischem Datenschutz“ geht es darum, wie ein Anbieter mit den erhobenen Daten umgeht. Gut ist, wenn er verspricht sie nicht zu nutzen. Schlecht ist, wenn er das nicht verspricht. Dann könnte er sie z.B. an andere verkaufen.
Es gibt noch mehr Möglichkeiten, deine Daten zu schützen.
Unter „Besonderheiten“ wird das erklärt.

Einfach gesagt!

Empfehlungen ausführlich erklärt



Auf den nachfolgenden Seiten werden Dienste aus drei Kategorien[8] entsprechend der vorab Beschriebenen Kriterien bewertet.

Messengerdienste

Hier werden alle Dienste die eher für den Austausch von Text-, Sprach- und Videonachrichten in Einzel- oder Gruppenchats ausgelegt sind aufgeführt und miteinander verglichen.

Kollaborationsdienste

Unter dieser Überschrift werden alle Dienste die prinzipiell für Telefonate, Videobesprechungen sowie den jederzeit möglichen Austausch von Textnachrichten und Dateien ausgelegt sind aufgeführt und miteinander verglichen.

Videokonferenzlösungen

Hierunter werden alle Dienste, die eher für reine Videobesprechungen genutzt werden, aufgeführt und miteinander verglichen.

Ein kurzer Exkurs: Die Mozilla Foundation (Hersteller von Firefox, Thunderbird, …) betreibt eine Webseite auf der sich Nutzer*innen über die Sicherheit von vernetzten Produkten informieren können (siehe [16]). Eine große Kategorie auf dieser Webseite bilden dabei Videoanruf Apps. Das hat zwei Vorteile. Erstens finden sich ein paar der betrachteten Dienste dort wieder, sodass die Bewertungen in diesem Ratgeber abgeglichen werden können. Zweitens führt die Webseite auch Bewertungen zu Diensten, die in diesem Ratgeber nicht betrachtet werden.

8 Die Zuordnung der Dienste zu den Kollaborationstools ist dabei nicht immer eindeutig, da viele Dienste zu ihrer Kernfunktionalität weitere Funktionen anbieten.



SIGNAL

★ ★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**



Signal nutzt für alle Einzel- und Gruppennachrichten, Sprachanrufe, Telefonate und Videoanrufe das Signal-Protokoll für die beste verfügbare Ende-zu-Ende Verschlüsselung [17] [18].
Zugleich arbeitet Signal „im Unterschied zu vielen anderen Messengern […] nach dem Zero-Knowledge-Prinzip, was bedeutet, dass der Anbieter selbst möglichst wenig über die Nutzer und darüber weiß, was sie auf der Plattform machen.“ [17] Konkret hat Signal technische Maßnahmen umgesetzt, um selbst nicht einmal zu wissen, wer mit wem kommuniziert. Nicht einmal die Telefonnummern verlassen die Geräte der Endanwender in einer lesbaren Form [17].



Eigentlich ist dieser Aspekt durch die technischen Maßnahmen irrelevant. Dennoch ist Signal auch hier vorbildlich: „Signal does not sell, rent or monetize your personal data or content in any way – ever“ [19]. Die übliche pauschale Ermächtigung personenbezogene Daten verarbeiten zu dürfen - im Sinne des „berechtigten Interesses“ - enthält die Datenschutzerklärung von Signal nicht. Korrekterweise, da Signal keine personenbezogenen Daten verarbeitet.



Die Implementierung erfolgt Open-Source und ist auf Github einsehbar. Dies ermöglichten Dritten Einsicht in die Implementierung, die Mitarbeit am Projekt und die präzisere Identifizierung um Meldung von etwaigen Sicherheitslücken.
Signal nutzt die Cloud-Infrastruktur großer amerikanischer Firmen. Dadurch wird es Regierungen erschwert die Kommunikation über Signal zu blockieren. Falls dies doch funktioniert, ermöglicht Signal den Betrieb eines Proxy-Servers, wodurch Nutzer*innen solche Blockaden umgehen können [20].
Signal erfordert zwar einen Desktop-Client, ermöglicht darüber aber auch das Teilen des Bildschirms. Gruppenanrufe sind mit max. 15 Personen möglich [21], sodass Signal den Bedarf nach Kollaborationsdiensten u. U. schon vollständig abdecken kann –wohlgemerkt bei vollständiger Ende-zu-Ende Verschlüsselung!

THREEMA

★ ★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

Threema bietet eine Ende-zu-Ende Verschlüsselung für Nachrichten an, setzt dabei aber auf eine proprietäre Umsetzung [22]. Genutzt wird die etablierte Bibliothek „NaCL“ sowie in Europa standardisierte Verschlüsselungsprotokolle. Dennoch sind sich Kryptographen einig, dass die Anwendung der einzelnen Protokolle insgesamt nicht die Sicherheit des Signal-Protokolls erreicht [18].
Threema versucht nach dem Zero-Knowledge-Prinzip auf Metadaten zu verzichten [23] und wirbt hierfür explizit damit auch ohne Telefonnummern und E-Mail-Adressen nutzbar zu sein. Zur Einordnung dieser Werbeaussage, ähnlich wie durch Signal begründet, ist die Angabe von diesen Daten hilfreich, damit möglichst viele Threema-Nutzer*innen wissen, dass man Threema nutzt und nicht auf unsichere Kommunikationsmittel wie SMS oder E-Mail ausweichen. So effektiv wie Signal ist das Zero-Knowledge-Prinzip allerdings nicht umgesetzt.

Entsprechend der Datenschutzerklärung, erhebt Threema Daten von Nutzer*innen nur um auf Supportanfragen antworten zu können [24].

Die Implementierung der Clients erfolgt Open-Source. Der Backend-Code ist Threemas Geheimnis. Als einziger Messenger in diesem Ratgeber, beauftragt Threema regelmäßig ein Audit des Quellcodes durch Dritte, um etwaige Probleme in der Umsetzung zu finden [25].
Threema betreibt lediglich zwei Datenzentren in Zürich. D. h. der Dienst ist anfällig gegen Naturkatastrophen [23].
Threema kennzeichnet Kontakte mit einer „Verifizierungsstufe“. Kontakte, die händisch abgeglichen worden sind, werden dabei in grün dargestellt. Kontakte, bei denen die Identität aufgrund des Kontaktbuchs (Telefonnummer/E-Mail) abgeglichen worden sind, sind in orange dargestellt. Kontakte, die rot gekennzeichnet sind, sollten nicht kontaktiert werden. Zumindest die Möglichkeit der Kontakt-Verifikation wurde mittlerweile u. a. von Signal und WhatsApp übernommen – da die Funktion hilft, sicherzustellen, dass man wirklich mit dem Endgerät der erwünschten Person kommuniziert.

WHATSAPP

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

WhatsApp schützt die Kommunikation von Daten mit dem Signal-Protokoll [26]. D.h. die Kommunikationsinhalte sind entsprechend der besten Ende-zu-Ende Verschlüsselung vor Zugriffen geschützt. Zudem entwickelt WhatsApp zurzeit die Möglichkeit die Backups zu verschlüsseln, sodass der bislang theoretisch mögliche Zugriff auf die Kommunikation durch Google bzw. Apple (Vertragspartner zur Ablage der Backups) bald nicht mehr möglich sein wird [27]. WhatsApp hat keine Maßnahmen etabliert, um Metadaten zu reduzieren (Zero-Knowledge-Prinzip).

WhatsApp führt die in Europa erfassten Daten in ihrer Datenschutzrichtlinie sehr detailliert auf. So „erhebt [WhatsApp] Informationen über deine Aktivität auf unseren Diensten“. Weiter „können [wir] mithilfe der von ihnen erhaltenen Informationen und sie können mithilfe der Informationen, die wir mit ihnen teilen, unsere Dienste bzw. ihre Angebote, einschließlich der Produkte von Facebook-Unternehmen, betreiben, bereitstellen, verbessern, verstehen, individualisieren, unterstützen und vermarkten. Dazu gehört: […] Personalisierungsfunktionen und Inhalte […] und das Anzeigen von relevanten Angeboten und Werbeanzeigen in den Produkten von Facebook-Unternehmen“ [28].

WhatsApp wird nicht Open-Source entwickelt.
WhatsApp hat sehr sinnvolle Funktionen integriert, die in vielen anderen Messengern fehlen. Z. B. ermöglicht WhatsApp die Erstellung von Stories, die 24h anderen Nutzern dargestellt werden. Zwar ist der Funktionsumfang nicht so weit ausgebaut wie beispielsweise bei Instagram, dafür ist die Reichweite über WhatsApp durch die deutlich höhere Nutzerzahl deutlich größer. Darüber hinaus bietet WhatsApp die Möglichkeit, Nachrichten durch Moderationen auf ihre Richtigkeit hin überprüfen zu lassen [29]. Dadurch werden u. U. vertrauliche Informationen mit WhatsApp geteilt [30] - was beim Weiterleiten von Nachrichten aber nicht verwundern sollte – dafür können Fake-News etc. einfacher erkannt werden.

TELEGRAM

★ ★

Geeignet für Daten der **Datenschutzklasse 1**

Telegram bietet zwar sogenannte Secret Chats an, die sind aber optional zu aktivieren, um eine Ende-zu-Ende Verschlüsselung zu nutzen. Secret Chats stehen darüber hinaus nur für die direkte Kommunikation zwischen zwei Nutzer*innen zur Verfügung. Gruppenchats können nicht Ende-zu-Ende verschlüsselt werden. Die genutzte Verschlüsselung (MTProto v2) wird nicht von Kryptographen empfohlen [18]. Zudem wurden erst jüngst Fehler im Protokoll gefunden [31]. Eine Transportverschlüsselung und Verschlüsselung ruhender Daten sind aber umgesetzt. Das schützt die Kommunikation vor Dritten, nicht aber vor der theoretischen Auswertung durch den Anbieter.
Der Schutz der Metadaten nach dem Zero-Knowledge-Prinzip wurde nicht umgesetzt, was aber bei dem technisch möglichen Zugriff auf die Kommunikation durch den Anbieter keinen Mehrwert bieten würde.

Telegram bezieht sich auf ihr berechtigtes Interesse (siehe DSGVO) um die Daten auf ihren Servern zu speichern. Eine Verarbeitung von Gesprächsinhalten geht aus der Datenschutzerklärung allerdings nicht explizit hervor. Allerdings sind Formulierungen wie: „We store messages, photos, videos and documents from your cloud chats on our servers so that you can access your data from any of your devices anytime without having to rely on third-party backups. All data is stored heavily encrypted and the encryption keys in each case are stored in several other data centers in different jurisdictions. This way local engineers or physical intruders cannot get access to user data.“ [32] nur ein Hinweis darauf, dass die Verschlüsselung ruhender Daten lokale Angriffe auf die Infrastruktur von Telegram unterbinden.

Telegram Clients werden Open-Source entwickelt. Die Serveranwendung nicht. Der Firmensitz von Telegram ist zurzeit in den Vereinigten Arabischen Emiraten.Telegram wurde in der Vergangenheit durch den Firmengründer finanziert. Ab 2021 soll die „Monetarisierung starten, um die Infrastruktur und die Gehälter der Entwickler finanzieren zu können. Das Erzielen von Gewinnen wie jedoch nie das Endziel von Telegram sein.“ [33]



FACEBOOK MESSINGER & INSTAGRAM-DIRECT

Geeignet für Daten der **Datenschutzklasse 0**

Anmerkung: In der Betrachtung werden beide Dienste zusammengefügt, da die Implementierung und die Datenschutzerklärung analog für beide Dienste gelten. Zudem plant Facebook seit langem die Vereinheitlichung beider Dienste.

Facebook Messenger bietet keine Ende-zu-Ende Verschlüsselung. Geplant ist eine Umsetzung frühestens in 2022 [34]. Eine Transportverschlüsselung ist umgesetzt. Ein etwaiger Schutz durch die Verschlüsselung ruhender Daten, kann nicht gezählt werden, da die Daten auf den Servern von Facebook aktiv ausgewertet werden.
Beide Dienste haben keine Maßnahmen etabliert, um Metadaten zu reduzieren (Zero-Knowledge-Prinzip).

Beide Dienste nutzen alle anfallenden Daten für automatisierte Auswertungen mit dem Ziel die Dienste zu personalisieren. Konkret bedeutet dies, dass Facebook die Daten u. a. für zielgerichtete Werbeprofile nutzt [35].

Die Implementierung erfolgt nicht Open-Source.
Instagram ermöglicht das Auffinden von Kontakten ohne Telefonnummer, E-Mail oder Threema-Id. Das kann sehr hilfreich sein, wenn man nach einem Workshop nur noch den Namen eines*r Teilnehmer*in kennt und nachträglich in Kontakt treten möchte.

SNAPCHAT

Geeignet für Daten der **Datenschutzklasse 0**

Snapchat hat wohl im Jahr 2019 eine Ende-zu-Ende Verschlüsselung für Snaps eingeführt. Memorys werden mittels des Passwortes der Nutzer*in verschlüsselt, bevor sie an Snapchat übermittelt wird. Leider verliert der Hersteller allerdings kein Wort bzgl. der genutzten Verschlüsselung und welche anderen Funktionen von Snapchat überhaupt verschlüsselt werden. Dadurch ist eine Bewertung dieses Aspektes nicht möglich.

Snapchat fordert für die Nutzung des Dienstes in ihrer Datenschutzerklärung eine sehr umfangreiche Liste an Daten an, die das Unternehmen mit Dritten teilt. Die Nutzung des Dienstes eignet sich daher nicht für vertrauliche Nachrichten [36].

Die Implementierung erfolgt nicht Open-Source.
Snapchat fordert auf seiner Webseite die Nutzer*innen auf: „Denk nach, bevor du einen Snap versendest und schick den Leuten nichts, was sie nicht bekommen wollen“ [37]. Dies ist ein grundsätzlich sinnvoller Ratschlag, v.a. da Snapchats größtes Probleme darin liegt, dass Nutzer*innen zu viel über sich preisgeben. Jedenfalls weist Snapchat mehrmals explizit darauf hin, dass es ein Irrglaube ist, dass mit Snapchat geteilte Nachrichten nach einer gewissen Zeit automatisch gelöscht und die Nachrichten nicht digital kopierbar sind. Auch wenn dasselbe grundsätzliche Problem bei vielen technischen Diensten analog existiert, könnte die Hauptursache darin liegen, dass vorzugsweise Jugendliche diesen Dienst nutzen.



ELEMENT

basierend auf Matrix

★ ★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**



Element bietet eine optionale Ende-zu-Ende Verschlüsselung jeglicher Kommunikationsinhalte an. Das zugrundeliegende Protokoll ist dabei stark an das Signal-Protokoll angelehnt. Zusätzlich ist Element auch durch eine Transportverschlüsselung und Verschlüsselung ruhender Daten abgesichert. Um auf alte Nachrichten auf einem neuen Gerät zugreifen zu können, müssen Nutzer*innen erst eine Verifikation durchführen. Dadurch wird der Schaden bei Zugangsdatendiebstählen minimiert.
Element scheint grundsätzlich bedacht nur benötigte Metadaten zu erfassen. Dies zeigt sich u. a., dass Element erst nach Zustimmung eine anonyme Datenerfassung umsetzt [38].



Element stellt eine gut verständliche und transparente Datenschutzerklärung aus. Aus dieser geht mitunter hervor, dass die eigentlichen Server von AWS gestellt und Schutzlösungen von Cloudflare genutzt werden [38]. Dadurch sind deren Datenschutzerklärungen grundsätzlich zwar auch relevant – aber technisch betrachtet können diese Anbieter eigentlich nur noch Daten erheben, die sie nutzen müssen (legitimes Interesse), um die Infrastruktur entsprechend zu betreiben (AWS) bzw. abzusichern (Cloudflare). Die Datenschutzerklärung von Element hingegen erläutert sehr gut, dass grundsätzlich nur wenige Daten und diese Zweckmäßig und auf Basis des legitimen Interesses von Element erhoben werden.



Element und das zugrundeliegende Matrix Protokoll werden beide Open Source entwickelt. Das ermöglicht u. a. den Betrieb auf der eigenen Infrastruktur.
Matrix wird u. a. von der französischen Regierung, der Bundeswehr und in der Verwaltung sowie Schulen von Schleswig-Holstein und Hamburg benutzt [39].
Der Betrieb der Server durch Element ist in Anbetracht der Kosten/Nutzen Bilanz ratsam. Nicht nur scheint Element hinsichtlich des Betriebes der Dienste sehr auf die Sicherheit zu achten, sondern zugleich bietet Element auch Lösungen um mit anderen Diensten wie Teams [40], Slack, Discord, Gitter, IRC und Telegram kompatibel zu sein [41]. Als einzige Lösung in diesem Ratgeber werden so die technischen Insellösungen vereinheitlicht.

ROCKET.CHAT

★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**

Rocket.Chat bietet eine Ende-zu-Ende Verschlüsselung für Nachrichten an. Zusätzlich ist Rocket.Chat durch eine Transportverschlüsselung abgesichert. Über eine Verschlüsselung ruhender Daten konnte keine Aussage gefunden werden (daher ein Stern Abzug).
Rocket.Chat hat keine Maßnahmen etabliert, um Metadaten zu reduzieren (Zero-Knowledge-Prinzip).

Rocket.Chat unterscheidet in ihrer Datenschutzerklärung zwischen dem Angebot welches auf den Servern von Rocket.Chat gehostet ist und selbst gehosteten Instanzen. Wenn Rocket.Chat selbst gehostet wird, bekommt Rocket.Chat keinerlei Daten. Wenn Rocket.Chat auf der Infrastruktur des Anbieters genutzt wird, werden Daten für den Betrieb des Dienstes erhoben. Ein Zugriff auf die Gesprächsinhalte räumt sich Rocket.Chat hingegen nicht ein [42].

Rocket.Chat wird Open Source entwickelt und kann auf der eigenen Infrastruktur gehostet werden.
Rocket.Chat bietet keine eigene Sprachanruf oder Videokonferenz Möglichkeit. Stattdessen gibt es eine Jitsi Meet Integration. Jitsi Meet ist in diesem Ratgeber als gesonderte Lösung aufgeführt.

MICROSOFT TEAMS

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**

Microsoft Teams bietet zurzeit keine Ende-zu-Ende Verschlüsselung. In Planung ist die Umsetzung einer solchen Verschlüsselung für Sprachanrufe [43]. Microsoft Teams ist aber Mittels Transportverschlüsselung sowie Verschlüsselung ruhender Daten abgesichert [44], sodass neben den Nutzer*innen nur der Anbieter Zugriff auf die Daten haben sollte. Alte TLS-Protokolle werden von Teams in ihren Cients nicht mehr unterstützt [45]. Teams Nutzer*innen werden per Active Directory eingeloggt. Konten können daher zentral durch eine 2-Faktor-Authentifizierung abgesichert werden, sodass der Schaden durch Zugangsdatendiebstählen minimiert wird. Teams setzt eine Datenresidenz entsprechend der geografischen Region ihrer Office 365 Organisation um [46].
Teams hat keine Maßnahmen etabliert, um Metadaten zu reduzieren (Zero-Knowledge-Prinzip).

Microsoft Teams erhebt entsprechend den Nutzungsbedingungen: Besprechungsinhalte, Aufzeichnungen, Profildaten und mehr [47]. Die Datenerhebung wird mit Verweis auf die Notwendigkeit für den Betrieb des Dienstes begründet.

Teams wird nicht Open-Source entwickelt.
Microsoft Teams war lange Zeit nur im Abo nutzbar. Während die private Nutzung seit ein paar Monaten über die mobilen Apps möglich ist, ist Teams zum 5. Oktober 2021 nun fester Bestandteil von Windows 11 & der Microsoft Office-Suite. Daher könnte die Nutzerschaft von Teams demnächst stark wachsen.
Microsoft Teams steht besonders in Baden-Württemberg im öffentlichen Fokus. Datenschützer zweifeln – wie bei vielen der, in diesem Ratgeber betrachteten, Dienste – an, dass die Datenschutzerklärung für Microsoft Teams einen Betrieb z. B. an Schulen zulässt. Hintergrund ist, dass Schulen, in ihrer Funktion als Verantwortliche Einrichtung nach der DSGVO, eigentlich ausführlich wissen müssen, wie Microsoft Teams die erhobenen Daten verarbeitet. Dies geht aus der Datenschutzerklärung von Microsoft Teams jedoch nicht hervor.



SLACK

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**



Slack bietet keine Ende-zu-Ende Verschlüsselung an und hat das auch nicht geplant. Slack setzt aktuelle Standards für die Transportverschlüsselung und Verschlüsselung ruhender Daten ein [48]. Alte TLS-Protokolle werden von Slack nicht mehr unterstützt [49]. Slack Konten können mit einer 2-Faktor-Authentifizierung abgesichert werden, sodass der Schaden durch Zugangsdatendiebstählen minimiert wird. Slack bietet Kunden die Möglichkeit, die Datenresidenz festzulegen.
Slack hat keine Maßnahmen etabliert, um Metadaten zu reduzieren (Zero-Knowledge-Prinzip).



Slack hebt in ihrer Datenschutzrichtlinie sehr stark ihre Bemühungen bzgl. der rechtskonformen Umsetzung von internationalen Datenübertragungen. Statt dies in separaten Dokumenten umzusetzen, wie z. B. bei Teams, wäre ein Fokus auf eine gute Beschreibung der eigenen Datenerhebung wünschenswert. Aus der Datenschutzrichtlinie ist nur zwischen den Zeilen herauszulesen, dass Slack und ggf. aktivierte Dienste von Dritten auf die Daten Zugriff haben, um u. a. „die Suchfunktion mithilfe von sonstigen Informationen [zu] verbessern, um das Ranking und die Relevanz von Inhalten, Channels oder Fachwissen für einen autorisierten Benutzer zu ermitteln, Vorschläge für Services oder Drittanbieterdienste basierend auf der historischen Nutzung und Vorhersagemodellen zu machen sowie organisatorische Trends und Erkenntnisse zu identifizieren, um so das Benutzererlebnis unserer Services anzupassen oder neue Produktivitätsfunktionen und Produkte zu kreieren.“ [50]. Slack räumt sich dadurch sehr weitgehende Befugnisse ein.



Slack wird nicht Open Source entwickelt.
An Slack Calls können maximal 15 Teilnehmer teilnehmen [51]. Eine Integration von Zoom ist in Slack möglich um Konferenzen mit mehr Nutzer*innen zu ermöglichen. Zoom ist in diesem Ratgeber als gesonderte Lösung aufgeführt.



DISCORD

★ ★

Geeignet für Daten der **Datenschutzklasse 1**



Discord bietet keine Ende-zu-Ende Verschlüsselung an und hat das auch nicht geplant. Discord setzt aktuelle Standards für die Transportverschlüsselung und Verschlüsselung ruhender Daten ein. Discord setzt zudem recht neue Konfigurationen wie HSTS Preloading ein, um den Aufbau der Transportverschlüsselung zusätzlich abzusichern. Disord Konten können mit einer 2-Faktor-Authentifizierung abgesichert werden, sodass der Schaden durch Zugangsdatendiebstählen minimiert wird.
Ein Zero-Knowledge-Prinzip wird bewusst nicht umgesetzt. Discord versteht sich als soziale Plattform und erlaubt mitunter die Einbindung von Facebook oder Twitter in das Discord Konto um Informationen über u. a. „Freunde“ und Kontakte mit Discord zu verknüpfen [52].



Discord räumt sich in ihrer Datenschutzerklärung Zugriff auf einige Daten ein. Als einer von wenigen Diensten in diesem Ratgeber bindet Discord auch die Twitter und Facebook SDKs in ihren Service ein, mit dem Ziel Informationen für „Werbekampagnen“ zu sammeln [52].
Verwunderlich ist, dass Discord in ihrer Datenschutzerklärung den Zugriff auf die Nutzerdaten nicht explizit aufführt. Discord scheint ein Problem mit Verletzungen ihrer Community Richtlinien zu haben. Laut ihrem „Transparenzbericht“ verwendet Discord automatisierte Tools, um u. a. Bilder von sexuellem Kindesmissbrauch zu finden [53]. Zudem hat Discords‘ Moderationsteam auch die Möglichkeit selbst auf „private Server“ zuzugreifen, wenn strafwürdige Inhalte gemeldet werden [54].



Discord wird nicht Open-Source entwickelt.
Discord basiert auf der Idee, eigene „Server“ für Communities zu betreiben. Physikalisch werden die Server weiterhin von Discord betrieben und verwaltet. Der technische Begriff wird von Discord hier zweckentfremdend. Grundidee, Nutzer*innen können selbst Communities erstellen, die mitunter auch viele 100.000 Nutzer*innen groß sind. Ähnlich zu Telegram, plagen Discord, durch diese Community-Räume bei über 140 Millionen Nutzer*innen, die in der Datenschutzerklärung bereits thematisierten Probleme bzgl. Richtlinien-Verstöße.



JITSI MEET

★ ★ ★ ★

Geeignet für Daten der **Datenschutzklasse 3**



Jitsi Meet bietet eine optionale, noch als experimentell gekennzeichnete Ende-zu-Ende Verschlüsselung an, durch die allerdings manche Funktionen deaktiviert werden. Da die virtuellen Besprechungsräume in Jitsi Meet standardmäßig nach dem Verlassen des letzten Nutzers gelöscht werden, müssen Nutzer*innen die Ende-zu-Ende Verschlüsselung jedes Mal neu aktivieren [55]. Jitsi Meet setzt aber auch eine Transportverschlüsselung und Verschlüsselung ruhender Daten ein. Konten müssen für Jitsi Meet nicht angelegt werden, der Zugang zu Besprechungen ist erstmal nur durch den Raumnamen geschützt und kann im laufenden Meeting durch ein Passwort weiter eingeschränkt werden.
Entsprechend der Datenschutzerklärung, erhebt Jitsi Meet wenige Metadaten, um den Betrieb der Services zu verbessern [56].



Die Datenschutzerklärung von Jitsi Meet ist vorbildlich kurz und schließt die Verwendung von Daten, außer für den technischen Betrieb der Plattform, aus. Darüber hinaus sichert die Datenschutzerklärung zu, dass Besprechungsinhalte wie Aufzeichnungen, wenn überhaupt, nur während der Besprechung vorgehalten werden [56].



Jitsi Meet wird Open-Source und explizit zum selbst hosten entwickelt [57]. Neben den offiziellen Servern, kann auch eine eigene Jitsi Meet Installation eingerichtet werden. Das ist nützlich, wenn garantiert keine Daten über die Server von 8x8, Inc. – der Firma hinter Jitsi – laufen sollen.
Im Falle einer 1:1 Besprechung über Jitsi Meet, wird eine Peer-to-Peer Verbindung aufgebaut. Dabei kommunizieren die Geräte der beiden Gesprächspartner*innen direkt miteinander – ohne dass der Jitsi Meet Server involviert wäre.
Jitsi Meet kennt eigentlich keine*n Moderator*innen. Mittlerweile gibt es aber auch „Jitsi Moderated Meetings“, welches zwei schwer erratbare Links für ein und dieselbe Besprechung erstellt. Für Gruppen, bei denen nicht ausgeschaltete Mikrophone problematisch sind, kann Jitsi Meet nun auch verwendet werden.

BIG BLUE BUTTON (BDKJ)

★ ★

Geeignet für Daten der **Datenschutzklasse 1**

BBB bietet keine Ende-zu-Ende Verschlüsselung an. Die BBB Instanz des BDKJs ist aber mittels einer Transportverschlüsselung gesichert. Bzgl. der Verschlüsselung ruhender Daten liegt keine Information vor. Moderatoren müssen sich anmelden, ein gesonderter Schutz der Nutzerkonten durch 2-Faktor-Authentifizierung ist nicht bekannt. Die Infrastruktur wird in Deutschland von der „Hetzner Online GmbH“ betrieben.
Eine BBB Anwendung kann sehr viele Metadaten über Sitzungen erfassen [58]. Ob diese Erfassung allerdings auch aktiv ist, ist unbekannt.

Hetzner Online GmbH sichert in ihrer Datenschutzerklärung zu, dass technische Logs in einer anonymisierten Form abgespeichert werden [59].
Der Betreiber der BBB-Instanz - IT-Abteilung des BDKJ/BJAs – stellt zurzeit keine Datenschutzerklärung aus.

Die BBB Anwendung selbst wird Open Source entwickelt.
Mittelfristig soll das Hosting der BBB-Instanz des BDKJ/BJAs, neben weiteren Diensten, bei fairkom erfolgen. Neben einer guten Absicherung der BBB Anwendung, bietet dies die Möglichkeit einer Auftragsverarbeitungsvereinbarung mit Fokus auf Datensparsamkeit. Eine solche Vereinbarung liegt aktuell noch nicht vor.

WICHTIG

BigBlueButton ist eine OpenSource entwickelte Anwendung. Die Anwendung an sich bringt keine Ende-zu-Ende Verschlüsselung mit, ist also auf eine Absicherung durch den Betreiber der BBB Anwendung angewiesen.
Der Betreiber der BBB Anwendung muss zudem die Datenschutzerklärung erstellen und veröffentlichen. Hierfür liefert BBB wertvolle Informationen [58]. BBB kann dabei so konfiguriert werden, dass nur wenige Interaktionen in den Besprechungsräumen und nur wenige weitere Metadaten erfasst werden. Unter letzterem fallen sicherlich u. a. IP-Adressen, um den Betrieb der Anwendung an sich gewährleisten zu können.

ZOOM

★ ★

Geeignet für Daten der **Datenschutzklasse 1**

Zoom bietet optional Ende-zu-Ende Verschlüsselung an, die auch im Nutzerprofil permanent aktiviert werden kann, durch die allerdings manche Funktionen deaktiviert werden. Zoom setzt eine Transportverschlüsselung ein. Bzgl. einer Verschlüsselung ruhender Daten liegen keine Information vor. Nutzerkonten können von Administratoren mittels 2-Faktor-Authentifizierung abgesichert werden, sodass der Schaden durch Zugangsdatendiebstählen minimiert wird. Die Teilnahme an Meetings kann allerdings auch anonym erfolgen. Der Zugang zu Meetings ist durch ein Passwort geschützt. Zahlende Nutzer*innen können eine Datenresidenz auswählen.
Zoom hat keine Maßnahmen etabliert, um Metadaten zu reduzieren (Zero-Knowledge-Prinzip).

Zoom räumt sich und Partnern in ihrer Datenschutzerklärung mit Bezug auf ihr berechtigtes Interesse weitreichende Rechte ein. Diese erstrecken sich auch auf Besprechungsinhalte, Kontakte, Profilinformationen, etc. [60]

Zoom wird nicht Open-Source entwickelt.
Zoom ist vielen erst dank der Pandemie bekannt, war es doch der Dienst, bei dem für viele Videokonferenzen auch stabil liefen. Erkauft war das besonders am Anfang der Pandemie durch zahlreiche, teils haarsträubende Fehler. Die bekanntesten dürften sicherlich der fehlende Schutz gegen das heute „Zoom-bombing“ genannte Problem und falsche Behauptungen bzgl. der Ende-zu-Ende Verschlüsselung sein. Eher technische Probleme wie Installer die teilweise mit Malware ausgeliefert wurden, Datenschutzpannen und etliche, teilweise kritische Sicherheitslücken, die bis heute in der Software gefunden werden, sind vmtl. nur in technischen Kreisen bekannt. An dieser Stelle, einen großen Dank an tomsguide, die eine stattliche Liste an Problemen chronologisch aufführen [61]. Mit dem Blick auf den heutigen Stand, muss anerkennend erwähnt werden, dass Zoom auf gemeldete Sicherheitsprobleme reagiert. Das alle Probleme aus der Welt geschafft sind, sollte noch nicht angenommen werden, sodass der Zoom Client regelmäßig aktualisiert werden sollte.



ZOOM ON-PREMISE (WGKD)

★ ★

Geeignet für Daten der **Datenschutzklasse 1**



Diese Zoom Variante enthält weithin nur eine optionale Ende-zu-Ende Verschlüsselung, bei der wieder manche Funktionen nicht zur Verfügung stehen. Der Unterschied zur normalen Zoom Version liegt allerdings darin, dass die Server für die eigentliche Videokonferenz (also nicht für die Nutzerprofile oder das Beitreten zu einer Konferenz) hier von einem Vertragspartner der Wirtschaftsgemeinschaft der Kirchen in Deutschland betrieben werden. Schutzmaßnahmen wir die Transportverschlüsselung und die Verschlüsselung ruhender Daten müssen dann von diesem Vertragspartner umgesetzt werden, was leider nicht überprüft werden konnte.
Metadaten wie Nutzerprofile, Teilnahme an Meetings, Nutzung des Zoomclients etc. können weiterhin von Zoom erfasst werden. Nur der Zugriff auf die Besprechungsinhalte ist für Zoom nicht mehr möglich.



Die Datenverarbeitung bzgl. der Besprechungsinhalte kann von der WGKD vertraglich mit dem Hoster geregelt werden. Die vertragliche Vereinbarung lag den Erstellern des Ratgebers aber nicht vor.

WEBEX

★ ★

Geeignet für Daten der **Datenschutzklasse 2**

WebEx bietet eine optionale Ende-zu-Ende Verschlüsselung an, bei der dann allerdings ein paar Funktionen aber auch WebEx-Geräte nicht mehr nutzbar werden. WebEx verspricht für Nutzerkonten, die nach 2018 angelegt worden sind, standardmäßig sowohl eine Transportverschlüsselung als auch eine Verschlüsselung ruhender Daten einzusetzen [62]. WebEx Nutzerkonten können mittels 2-Faktor-Authentifizierung abgesichert werden, sodass der Schaden durch Zugangsdatendiebstählen minimiert wird. Die Teilnahme an Meetings kann allerdings auch anonym erfolgen. Der Zugang zu Meetings ist durch ein Passwort geschützt. Durch Nutzer generierte Daten werden in dem Datenzentrum gespeichert, welches sich am „nächsten“ am Ort der Nutzer*in befindet. Das wäre sehr wahrscheinlich in Frankfurt [62]. Allerdings werden Rechnungsdaten und Analysedaten von WebEx in den USA gespeichert [62] [63]. Für kostenfreie Nutzerkonten behält sich WebEx allerdings vor, dass die Daten auch in ganz anderen Rechenzentren gespeichert sein könnten. [62]
In der Datenschutzerklärung werden etliche Daten und Metadaten aufgeführt. Im Vergleich zu Mitbewerber*innen wird die Datenerhebung jeweils begründet, sodass nachvollziehbarer ist, warum welche Daten erhoben werden. Allerdings bleibt intransparent, wie die Verarbeitung konkret aussieht [62]. Manche der Daten scheinen zudem noch einsparbar zu sein, ein Zero-Knowledge-Prinzip ist also nicht gegeben.

WebEx ist zwar vorbildlich transparent, welche Daten sie erheben und warum sie dies tun. Allerding verarbeitet WebEx viele personenbezogene Daten, einschließlich der Besprechungsinhalte [62].

WebEx wird nicht Open-Source entwickelt.

WEBEX (DRS)

★ ★ ★

Geeignet für Daten der **Datenschutzklasse 2**

Siehe WebEx.

Siehe WebEx.

Es können eigentlich keine Unterschiede zur normalen Variante ausgemacht werden. Sehr wahrscheinlich dürfte vertraglich die Speicherung der Daten in Frankfurt vereinbart worden sein. Davon unbetroffen werden die Zahlungsdaten und Analysedaten in den USA verarbeitet, da WebEx hier keine andere Regelung anbietet.
Vorteil der DRS Variante wird aber sicherlich die zentrale Verwaltung von mitunter datenschutzrelevanten Optionen von WebEx sein. Konkrete Einstellungen sind zum Zeitpunkt der Bewertung allerdings nicht bekannt. Eine standardmäßige Ende-zu-Ende Verschlüsselung wäre beispielsweise eine solche Option.

VERWEISE



[1] „Datenschutz-Grundverordnung,“ [Online]. Available: https://dsgvo-gesetz.de/. [Zugriff am 21 09 2021].
[2] „Kirchliches Amtsblatt für die Diözese Rottenburg-Stuttgart,“ 05 03 2018. [Online]. Available: https://datenschutz.drs.de/fileadmin/user_files/237/Gesetze/Kirchliches_Amtsblatt_2018_Nr._04__069-096_.pdf. [Zugriff am 10 10 2021].
[3] „Datenschutz-Grundverordnung,“ 25 05 2018. [Online]. Available: https://dsgvo-gesetz.de/. [Zugriff am 10 10 2021].
[4] „Im Inner Circle - Terroristen und Kriminelle ändern ihre Art der Kommunikation. Also müssen wir auch anders denken.,“ [Online]. Available: https://www.bnd.bund.de/DE/Die_Themen/Stories/SOCMINT/socmint_node.html. [Zugriff am 10 10 2021].
[5] A. Meister, „Bundesnachrichtendienst erhält so viele Überwachungsbefugnisse wie noch nie,“ Netzpolitik.org, 26 03 2021. [Online]. Available: https://netzpolitik.org/2021/bnd-gesetz-bundesnachrichtendienst-erhaelt-so-viele-ueberwachungsbefugnisse-wie-noch-nie/. [Zugriff am 10 10 2021].
[6] „MASSENÜBERWACHUNG & PRIVATSPHÄRE,“ amnesty, [Online]. Available: https://www.amnesty.de/informieren/themen/massenueberwachung-privatsphaere. [Zugriff am 10 10 2021].
[7] D. Berger, „Instagram: Werbefirma griff massenhaft Daten ab,“ heise online, 08 08 2019. [Online]. Available: https://www.heise.de/newsticker/meldung/Instagram-Werbefirma-griff-massenhaft-Daten-ab-4490717.html. [Zugriff am 10 10 2021].
[8] H. Wieler, „Insider Threats: Die Gefahr von Innen wird nach wie vor unterschätzt,“ Infopoint Security, 09 08 2021. [Online]. Available: https://www.infopoint-security.de/insider-threats-die-gefahr-von-innen-wird-nach-wie-vor-unterschaetzt/a28379/. [Zugriff am 10 10 2021].
[9] „Was Social-Media-Nutzer über ihr Privatleben verraten,“ Süddeutsche Zeitung, 10 07 2018. [Online]. Available: https://www.sueddeutsche.de/digital/twitter-studie-privatsphaere-nutzer-1.4047115. [Zugriff am 10 10 2021].
[10] „Cybermobbing unter Schülern,“ Betzold, 13 06 2019. [Online]. Available: https://www.betzold.de/blog/cybermobbing/. [Zugriff am 10 10 2021].
[11] „Jugend und Handy - Ständig vernetzt mit Smartphone & Co,“ [Online]. Available: https://www.medien-in-die-schule.de/unterrichtseinheiten/jugend-und-handy/modul-2-cybermobbing-und-anderes-problematisches-verhalten/. [Zugriff am 10 10 2021].
[12] „Identitätsdiebstahl durch Datenleaks und Doxing,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html. [Zugriff am 10 10 2021].
[13] „IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen,“ [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Kandidierende.pdf?__blob=publicationFile&v=7. [Zugriff am 26 09 2021].
[14] D. Schirrmacher, „Android 6.0: Vollverschlüsselung ab Werk für ausgewählte Geräte,“ 20

10 2015. [Online]. Available: https://www.heise.de/security/meldung/Android-6-0-Vollverschluesselung-ab-Werk-fuer-ausgewaehlte-Geraete-2851321.html. [Zugriff am 26 09 2021].
[15] J. Schmidt, „iOS-Verschlüsselung durchleuchtet," 17 12 2013. [Online]. Available: https://www.heise.de/security/artikel/iOS-Verschluesselung-durchleuchtet-2066500.html. [Zugriff am 26 09 2021].
[16] „Be Smart. Shop Safe.," Mozilla Foundation, [Online]. Available: https://foundation.mozilla.org/en/privacynotincluded/categories/video-call-apps/. [Zugriff am 05 10 2021].
[17] M. T. u. S. Grüner, „Warum es okay ist, dass Signal Google-Server nutzt," 29 01 2021. [Online]. Available: https://www.golem.de/news/whatsapp-alternative-warum-es-okay-ist-dass-signal-google-server-nutzt-2101-153764.html. [Zugriff am 27 09 2021].
[18] „Sichere Messenger: WhatsApp und Alternativen im Test," ct.21.08, pp. 14-19, 27 03 2021.
[19] „Signal Terms & Privacy Policy," [Online]. Available: https://www.signal.org/legal/. [Zugriff am 27 09 2021].
[20] S. Grüner, „Mit dem eigenen Signal-Proxy gegen staatliche Zensur," 05 02 2021. [Online]. Available: https://www.golem.de/news/whatsapp-alternative-mit-dem-eigenen-signal-proxy-gegen-staatliche-zensur-2102-153952.html. [Zugriff am 27 09 2021].
[21] „Gruppenanrufe - Sprache oder Video mit Bildschirmfreigabe," Signal, [Online]. Available: https://support.signal.org/hc/de/articles/360052977792-Gruppenanrufe-Sprache-oder-Video-mit-Bildschirmfreigabe. [Zugriff am 10 10 2021].
[22] „Cryptography Whitepaper," 21 06 2021. [Online]. Available: https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf. [Zugriff am 03 10 2021].
[23] „Merkblatt Sicherheit & Datenschutz," 27 07 2020. [Online]. Available: https://threema.ch/docs/work/threema_privacy-security_de.pdf. [Zugriff am 03 10 2021].
[24] „Datenschutzerklärung," 26 05 2021. [Online]. Available: https://threema.ch/de/privacy. [Zugriff am 03 10 2021].
[25] „Wie erfolgt die Sicherheitsprüfung bei Threema?," [Online]. Available: https://threema.ch/de/faq/code_audit. [Zugriff am 03 10 2021].
[26] „WhatsApp Encryption Overview," 22 10 2020. [Online]. Available: https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=0Ibe01sfaYsAX_wp3rL&_nc_ht=scontent.whatsapp.net&oh=3e733be5cc12cb509762ac19bd93252f&oe=615F5D99. [Zugriff am 03 10 2021].
[27] „Security of End-To-End Encrypted Backups," 10 09 2021. [Online]. Available: https://www.heise.de/downloads/18/3/1/6/7/3/1/1/WhatsApp_Security_Encrypted_Backups_Whitepaper.pdf. [Zugriff am 03 10 2021].
[28] „WhatsApp Datenschutzrichtlinie," [Online]. Available: https://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies. [Zugriff am 03 10 2021].
[29] S. Grüner, „1.000 Moderatoren prüfen gemeldete Whatsapp-Nachrichten," 08 09 2021. [Online]. Available: https://www.golem.de/news/messenger-1-000-moderatoren-pruefen-gemelde-

te-whatsapp-nachrichten-2109-159434.html. [Zugriff am 03 10 2021].
[30] P. Wagenseil, „WhatsApp is still safe to use, despite story claiming otherwise," [Online]. Available: https://www.tomsguide.com/news/facebook-whatsapp-propublica. [Zugriff am 03 10 2021].
[31] J. Schmidt, „Forscher decken Fehler in Telegrams Verschlüsselung auf," 09 07 2021. [Online]. Available: https://www.heise.de/news/Forscher-decken-Fehler-in-Telegrams-Verschluesselung-auf-6140917.html. [Zugriff am 21 09 2021].
[32] „Telegram Privacy Policy," [Online]. Available: https://telegram.org/privacy. [Zugriff am 27 09 2021].
[33] „Wie wird Telegram Geld verdienen?," [Online]. Available: https://telegram.org/faq#f-wie-wird-telegram-geld-verdienen. [Zugriff am 27 09 2021].
[34] „Messenger Policy Workshop: Future of Private Messaging," 30 04 2021. [Online]. Available: https://about.fb.com/news/2021/04/messenger-policy-workshop-future-of-private-messaging/. [Zugriff am 03 10 2021].
[35] „Instagram-Datenschutzrichtlinie," [Online]. Available: https://help.instagram.com/519522125107875. [Zugriff am 03 10 2021].
[36] „Datenschutzerklärung," Snapchat, 30 09 2021. [Online]. Available: https://www.snap.com/de-DE/privacy/privacy-policy. [Zugriff am 04 10 2021].
[37] „Snapchat Sicherheitscenter," Snapchat, [Online]. Available: https://www.snap.com/de-DE/safety/safety-center. [Zugriff am 04 10 2021].
[38] „Privacy policy," Element, [Online]. Available: https://element.io/privacy. [Zugriff am 09 10 2021].
[39] H. Bielawa, „Slack-Konkurrent gewinnt Auftrag für Bildung und Verwaltung in Deutschland," t3n, 18 07 2020. [Online]. Available: https://t3n.de/news/slack-konkurrent-gewinnt-auftrag-1299881/. [Zugriff am 09 10 2021].
[40] „EMS launches bridging for Microsoft Teams," 14 04 2021. [Online]. Available: https://element.io/blog/ems-launches-bridging-for-microsoft-teams/. [Zugriff am 09 10 2021].
[41] „Pricing," Element, [Online]. Available: https://element.io/pricing. [Zugriff am 09 10 2021].
[42] „Privacy Policy," Rocket.Chat Technologies Corp., 23 10 2020. [Online]. Available: https://docs.rocket.chat/legal/privacy. [Zugriff am 10 10 2021].
[43] T. Warren, „Microsoft Teams is getting end-to-end encryption support," 02 03 2021. [Online]. Available: https://www.theverge.com/2021/3/2/22308915/microsoft-teams-end-to-end-encryption-support-e2ee. [Zugriff am 03 10 2021].
[44] „Security and Microsoft Teams," Microsoft, 15 10 2020. [Online]. Available: https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide. [Zugriff am 10 10 2021].
[45] „UPDATE: Transport Layer Security 1.0 and 1.1 disablement," Microsoft, 24 08 2021. [Online]. Available: https://docs.microsoft.com/en-us/lifecycle/announcements/transport-layer-security-1x-disablement. [Zugriff am 10 10 2021].
[46] „Speicherort von Daten in Microsoft Teams," Microsoft, 29 07 2021. [Online]. Available:

https://docs.microsoft.com/de-de/microsoftteams/location-of-data-in-teams. [Zugriff am 10 10 2021].
[47] „Datenschutz und Microsoft Teams," [Online]. Available: https://docs.microsoft.com/de-de/microsoftteams/teams-privacy. [Zugriff am 03 10 2021].
[48] „Security at Slack," Slack. [Online]. Available: https://a.slack-edge.com/964df/marketing/downloads/security/Security_White_Paper_2020.pdf. [Zugriff am 10 10 2021].
[49] „Deprecating TLS v1.0 and v1.1," Slack, 27 02 2020. [Online]. Available: https://api.slack.com/changelog/2019-07-deprecate-early-tls-versions. [Zugriff am 10 10 2021].
[50] „Datenschutzrichtlinie," Slack, [Online]. Available: https://slack.com/intl/de-de/trust/privacy/privacy-policy. [Zugriff am 10 10 2021].
[51] „Effizientere Online-Meetings mit Video-Konferenzen," Slack, [Online]. Available: https://slack.com/intl/de-de/video-conferencing. [Zugriff am 10 10 2021].
[52] Discord, „DISCORD PRIVACY POLICY," 23 06 2020. [Online]. Available: https://discord.com/privacy. [Zugriff am 08 10 2021].
[53] „Discord Transparency Report: July — Dec 2020," Discord, 03 04 2021. [Online]. Available: https://blog.discord.com/discord-transparency-report-july-dec-2020-34087f9f45fb. [Zugriff am 08 10 2021].
[54] E. Kühl, „Discord - Der heißeste Chatdienst seit WhatsApp," Zeit Online, 14 04 2021. [Online]. Available: https://www.zeit.de/digital/internet/2021-04/discord-chat-plattform-microsoft-uebernahme-app/komplettansicht. [Zugriff am 08 10 2021].
[55] „Jitsi Meet Security & Privacy," [Online]. Available: https://jitsi.org/security/. [Zugriff am 09 10 2021].
[56] „meet.jit.si Privacy Supplement," 8x8, Inc., [Online]. Available: https://jitsi.org/meet-jitsi-privacy/. [Zugriff am 09 10 2021].
[57] „Jitsi-Meet," [Online]. Available: https://github.com/jitsi/jitsi-meet. [Zugriff am 09 10 2021].
[58] „Privacy," BigBlueButton, [Online]. Available: https://docs.bigbluebutton.org/admin/privacy.html. [Zugriff am 09 10 2021].
[59] „HETZNER ONLINE GMBH DATENSCHUTZERKLÄRUNG," Hetzner Online GmbH, [Online]. Available: https://www.hetzner.com/de/rechtliches/datenschutz. [Zugriff am 09 10 2021].
[60] „Zooms Datenschutzerklärung," Zoom, 04 06 2021. [Online]. Available: https://explore.zoom.us/docs/de-de/privacy.html. [Zugriff am 06 10 2021].
[61] P. Wagenseil, „Tom's Guide is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Learn more," [Online]. Available: https://www.tomsguide.com/news/zoom-security-privacy-woes. [Zugriff am 06 10 2021].
[62] C. WebEx, „Privacy Data Sheet - Cisco Webex Meetings," 09 2021. [Online]. Available: https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf. [Zugriff am 08 10 2021].
[63] „Where are the Webex Data Centers and iPOP Locations?," WebEx, 01 09 2021. [Online].

Available: https://help.webex.com/en-US/article/WBX28754/Where-are-the-Webex-Data-Centers-and-iPOP-Locations?. [Zugriff am 08 10 2021].
[64] „Gesetz über den Kirchlichen Datenschutz," [Online]. Available: https://katholische-kirche-leinefelde.de/fileadmin/Dateien_Oeffentlich/Gesetz_ueber_den_kirchlichen_Datenschutz.pdf. [Zugriff am 21 09 2021].
[65] M. Holland, „Ex-NSA-Chef: „Wir töten auf Basis von Metadaten"," 12 05 2014. [Online]. Available: https://www.heise.de/newsticker/meldung/Ex-NSA-Chef-Wir-toeten-auf-Basis-von-Metadaten-2187510.html. [Zugriff am 26 09 2021].
[66] „We're changing communication to be open for anyone to connect with everyone.," Element, [Online]. Available: https://element.io/about. [Zugriff am 09 10 2021].