Liste verschiedener Digitalplattformen

Arbeitshilfe für Selbsthilfegruppen und -initiativen

SHZ Selbsthilfezentrum München

Stand 7. April 2020

Inhalt:

Eingangsbemerkung:

Alle Welt ist in der aktuellen Coronaviruskrise nun dabei, sich online/digital zu vernetzen. Es werden Telefon- und Videokonferenzen abgehalten, Co-Working-Tools und Chatplattformen genutzt, was natürlich eine sinnvolle Alternative zum Face-to-Face-Austausch ist. Leider wird dabei der Datenschutz meist nicht ausreichend oder gar nicht (mehr?) berücksichtigt.

Die folgende Auflistung soll echte Alternativen aufzeigen, die dem Schutz der persönlichen Daten Rechnung tragen (kein Tracking, kein Google-Analytics, keine Weitergabe der gesammelten Daten an Dritte etc.) und auch für „Laien“ gut handhabbar sind. Denn wenn man sich intensiv mit diesem sehr weiten Feld befasst, kommt man zu dem Schluss, dass es hier, für unsere Anliegen, keinen „Königsweg“, keine zu 100 % empfehlenswerten Lösungen gibt – diese gäbe es zwar prinzipiell, aber man muss entweder Abstriche bei der Qualität hinnehmen oder ein versierter IT-Spezialist sein.

Diese Liste ist vorläufig und wird laufend aktualisiert und verbessert.
Wer Hinweise, Kommentare oder Anmerkungen hat, möge sich bitte melden (siehe unten).

Alle hier genannten Informationen stammen aus eigener Recherche, von uns bekannten IT-Spezialisten oder folgenden Internetseiten, auf denen weitere sehr interessante und sehr kompetent wirkende Hinweise zu finden sind:

https://www.kuketz-blog.de/
https://digitalcourage.de/blog/2020/corona-homeoffice-tipps#2

Vom Kuketz-Blog stammt dieser dieser Eintrag vom 30. März 2020 | 18:06 Uhr

> Corona und die »Nebenwirkungen« beim Datenschutz
> Aktuell erhalte ich viele Meldungen von Lesern, die sich darüber beschweren, wie der Datenschutz in Zeiten von Corona gerade in Vergessenheit gerät. Schulen, deren Lehrer die Schüler in einer WhatsApp-Gruppe versammeln, um ihnen Aufgaben zukommen zu lassen. Unternehmen, die auf Zoom zurückgreifen, um Videokonferenzen durchzuführen. Behörden, die die Bürger dazu aufrufen, sensible Dokumente via Microsoft Office Lens (Link führt zum Play Store) einzusenden. Das sind nur ein paar Beispiele, die aufzeigen, wie schlimm die Lage ist – und zwar nicht nur im Gesundheitswesen.
> Es ist erstaunlich, wie unvorbereitet die meisten Verantwortlichen in solch einer Krise sind. Noch schlimmer ist allerdings die Tatsache, wie »kopflos« in Sachen Datenschutz gerade agiert wird. Wird sich nach der Corona-Krise etwas ändern? Vielleicht dann, wenn das Thema Datenschutz in Deutschland als Chance und nicht als »Digitalisierungsverhinderer« verstanden wird.

Videokonferenzen

Ein allgemeiner Hinweis: Videokonferenzen benötigen immer eine gute Internetverbindung. Gerade in diesen Zeiten, in denen sich alle digital vernetzen, sind die Übertragungswege generell einer hohen Belastung ausgesetzt, so dass es unabhängig vom Anbieter oder den jeweils individuellen technischen Vorraussetzungen immer wieder zu Störungen kommen kann.

Manchmal liegt es aber auch in der Tat am eigenen Anschluss, denn etliche Anbieter von Telefon- bzw. Internetverbindungen werben zwar mit einer hohen Downloadrate, die beim Surfen durch das Internet auch völlig ausreichend ist. Bei Videokonferenzen (oder allgemein interaktiven Anwendungen) kommt es aber auch auf eine ausreichende Upload-Rate an – und die sollte für einen ruckelfreien Betrieb mindestens 10 MBit/s betragen.

Bei schlechter Verbindungsqualität hilft es manchmal auch, die Bildschirmauflösung zu verringern oder die Kamera ganz auszuschalten. Dann gibt es zwar keine Bildübertragung mehr, aber das ist dann vielleicht das kleinere Übel.

✶ Jitsi Meet

Obwohl Jitsi auf den ersten Blick wie eine Anwendung für Computernerds daherkommen mag, empfehlen wir das Angebot trotzdem, denn es ist im Grunde leicht handhabbar und vor allem aus Datenschutzsicht unbedenklich.
Es ist eine Open-Source-Software, die kostenlos ist und keine Registrierung erfordert, die Daten werden nicht gespeichert und verkauft
Voraussetzung ist ein Browser mit WebRTC-Unterstützung z.B. Firefox oder Chrome/Chromium (wobei die letzteren zwar eine bessere Performance haben, aber aus unserer Sicht dennoch nicht empfehlenswert sind, da beide Browser Google-Anwendungen sind).
Bei Nutzung mit dem Smartphone braucht man die **Jitsi Meet** App für Android oder iOS.

Nach dem Aufrufen der Website
https://meet.adminforge.de/
muss man einen Server auswählen, einen Namen für das eigene Meeting eintragen und auf „LOS“ klicken. Der Zugriff auf die eigene Kamera und das Mikrofon muss erlaubt werden. Dann kann man weitere Teilnehmer einladen und erhält einen Link mit Passwort. Beides schickt man per E-Mail an die entsprechenden Teilnehmer*innen.

Diese Anleitung ist etwas ausführlicher auch hier:
https://adminforge.de/tools/videokonferenzen-mit-jitsi-meet/

Unsere Erfahrung:
Es ist hinzuzufügen, dass diese Plattform bei vielen Teilnehmer*innen an ihre Grenzen zu kommen scheint. Unser Versuch mit 11 Teilnehmer*innen war leider nicht sehr erfolgreich.

✶ Blizz

Blizz gehört zur Team-Viewer-Familie und scheint nach jetzigem Kenntnisstand datenschutzrechtlich unbedenklich, der Server steht in Deutschland, die AGBs erscheinen transparent.

https://www.blizz.com/de/

Über Blizz kann man sich mit Bild, ohne Bild oder auch per Telefon treffen Das Angebot ist bis zu 5 Teilnehmer*innen (TN) kostenlos. Danach sind gestaffelt (bis 10, bis 25 etc. TN) monatliche Beträge bis maximal 19,95 € zu zahlen. Eine Person bestellt und bezahlt dieses Angebot und die anderen TN können sich ohne Registrierung mit der Meeting-Id (und gegebbnnflls. Passwort) einwählen.

Es ist hinzuzufügen, dass diese Plattform den Download eines Programms erfordert, das wiederum an bestimmte Systemvoraussetzungen geknüpft ist. D.h., dass Blizz mit älteren Betriebssystemen oder Browserversionen nicht nutzbar ist.

Nach dem Download und der Installation der Software kann man mit Klick auf den grünen Button ein eigenes Meeting starten (oder an einem bestehenden teilnehmen, wenn die Meeting-Id bekannt ist). Dann erhält man eine Meeting-Id, die man an die Teilnehmer*innen per Mail versenden kann. Die Bedienung der Software wird erklärt, wenn man „So funktioniert's" aufruft.

- **talky**

Eine wirklich gute Alternative – für kleine Gruppen bis zu 6 Teilnehmer*innen – scheint nach jetzigem Kenntnisstand ein noch relativ unbekannter Dienst zu sein, der mit Jitsi-Servern zusammenarbeitet. Die Datenschutzbestimmungen scheinen sehr gut eingehalten zu werden und auch die Übertragungsqualität lässt kaum zu wünschen übrig. Allerdings ist dieses Angebot nur auf englisch zu haben, was manche abschrecken wird. Wir ermutigen, es dennoch zu probieren, denn eigentlich ist alles gut verständlich.

www.talky.io

Wir versuchen es hier mal mit einer Anleitung:
Nach dem Aufrufen der Website gibt man in den Kasten nach „talky.io/….." einen Namen für die Konferenz ein (wenn man mehrmals draufklickt, wird einem auch ein Phantasiename angeboten). Dann „Start a chat" anklicken und man kommt man auf eine Seite, auf der man den Zugriff auf Kamera und Mikrofon erlauben muss: „Allow camera access" und „Allow microphone access". Dann öffnet sich wahrscheinlich noch ein Fenster des eigenen Computers, wo man das ebenfalls erlauben muss – wenn alles geklappt hat, sieht man sich selber.
Danach „Join call" anklicken. Auf der nächsten Seite sieht man sich links in der schmalen Leiste (dort kann man über dem eigenen Bild noch einen Namen für sich vergeben) und oben steht auf blauem Grund „Invite". Darauf klicken, um andere zu dem Meeting einzuladen.
Dann steht in diesem Feld „Copied Link!", was bedeutet, dass der Einladungslink in die Zwischenablage kopiert wurde (das ist bei jedem Computer ein versteckter Speicherort, dessen Inhalt man mit „Einfügen" in jedes Dokument/Programm einfügen kann). Auf diese Weise kann man diesen Link in eine E-Mail einfügen, um ihn den Teilnehmer*innen zu schicken.

Vorher kann man sich noch entscheiden, ob das Meeting mit einem Passwort geschützt ablaufen soll. Wenn ja, dann muss man unter dem blauen „Invite"-Button rechts noch den grauen Button „Lock" anklicken. Dann erscheint über dem blauen „Invite"-Button „Room Locked: ????", und diese 4 Ziffern muss man den Teilnehmer*innen ebenfalls mitteilen.

Die müssen nach Aufrufen des Links ebenfalls den Zugriff auf Kamera und Mikrofon erklauben und werden dann zum Meeting dazugeschaltet.

Während des Meetings kann man unter dem eigenen Bild links mit den beiden Buttons Mikrofon oder Kamera vorübergehend ab- und dann wieder anschalten. Mit dem Button daneben „Share screen" kann man den eigenen Bildschirm für die anderen freigeben, um ein Dokument oder Foto oder was auch immer vom eigenen Computer den anderen zu zeigen. Wenn man darauf klickt, dann

erscheint ein eigenes kleines Fenster, mit dem man das entsprechende Fenster (den Bildschirm) auswählen kann, das man den anderen zeigen möchte (das muss natürlich bereits geöffnet sein, was man aber auch während des Meetings öffnen kann, ohne es zu verlassen).

Danach kann man links unter dem eigenen Bild die Freigabe wieder zurücknehmen: „stop sharing".

Rechts unten ist noch ein Button „chat". Wenn man den anklickt, öffnet sich ein kleines Fenster, in das man Textnachrichten schreibt, die dann von allen gelesen werden können (wenn das Häkchen bei „Send as I type" gesetzt ist, dann können alle das Eintippen direkt verfolgen).

Das Meeting kann man mit dem Button „Leave" verlassen (links unter dem blauen „Invite-Button").

Telefonkonferenzen

Ein allgemeiner Hinweis: Es kann vorkommen, dass man bei Telefonkonferenzen einen Hall oder ein Echo hört. Das kann sehr störend sein. Wir empfehlen trotzdem, die Konferenz nicht aufzugeben, denn meistens verschwindet das nach einer gewissen Zeit wieder. Wer die Möglichkeit hat, sollte es auch mal mit einem Headset versuchen, das kann oft helfen.

- **Deutsche Telefonkonferenz:**

Dieser Anbieter erscheint seriös und transparent. Die Nutzung ist denkbar einfach: auf der Website den Button „Kostenlos starten" anklicken, dann gibt man seine E-Mail-Adresse und den Sicherheitscode ein, muss auch noch das Häkchen bei der Zustimmung zu den AGBs etc. setzen, danach erhält man die Zugangsdaten in sein E-Mail-Postfach und kann damit andere Teilnehmer*innen einladen.

Wegen der zur Zeit hohen Auslastung ist die Registrierung und/oder Einwahl zeitweise nicht möglich – dann passiert beim Klick auf „Jetzt starten!" gar nichts. Wenn man bereits registriert ist, empfiehlt sich eine Verabredung zu einer „krummen" Uhrzeit (z.B. 9.24 Uhr und nicht 9.30 Uhr).

https://www.deutsche-telefonkonferenz.de

- **Meebl**

Dieser Anbieter hat ebenfalls sehr transparente Nutzungsbedingungen und weist darauf hin, dass Facebook- und Google-Implementierungen enthalten sind. Insofern empfehlen wir meebl nicht so uneingeschränkt, halten es aber für vertretbar, wenn bei der Nutzung bzw. Registrierung über einen Computer oder das Smartphone alle Facebook- und Google-Anwendungen geschlossen sind. Daher empfehlen wir auch, nicht das Einladungstool auf der Seite zu nutzen, sondern die Teilnehmer*innen über den eigenen E-Mail-Account einzuladen und in die E-Mail die Einwahldaten hineinzukopieren.

Die Registrierung ist ebenfalls einfach: Auf der Website die E-Mail-Adresse und den Sicherheitscode eingeben. Dann erhält man Zugang zu einem Konferenzraum mit den dazugehörigen Daten. Dieser ist dann für 3 Tage reserviert. D.h., dass die Einladung der anderen Teilnehmer*innen nicht sehr lange im Voraus erfolgen kann.

https://www.meebl.de

- **mumble**

Dieses Angebot ist zum einen nur in englisch zu haben und benötigt zum anderen den Download eines Programms, das auf der Website abrufbar ist. Insgesamt erscheint und diese Option als etwas kompliziert, so dass wir sie nicht unbedingt empfehlen. Dennoch kann es eine Alternative sein, wenn die anderen Anbieter überlastet sind.

https://www.mumble.info/

Erläuterungen auf deutsch gibt's hier:
https://wiki.freifunk.net/Mumble

Messenger-Dienste:

- Wire (offenbar nicht mehr empfehlenswert?)

Dieser Anbieter wird landläufig als Alternative zu WhatsApp bezeichnet. Leider sind die Eigentumsverhältnisse heute nicht mehr die der Ursprungsidee: Ende Juli 2019 wurde die Wire Swiss GmbH von der Wire Group Holdings Inc. (Dover, USA) übernommen. Der Eigentümer des Unternehmens befindet sich demnach in den USA.

Es ist nicht eindeutig ersichtlich, ob und welche datenschutzrechtlichen Bedenken sich daraus ergeben. Allerdings kann man schon jetzt sagen, dass eine Datenbank mit Klartext-Metadaten geführt wird. Die Wire-Server speichern in einer Datenbank-Tabelle Informationen darüber, wer mit wem wann kommuniziert – im Klartext: damit unterscheidet sich das Proteus-Protokoll signifikant vom Signal-Protokoll, das Wert auf die Vermeidung von Metadaten legt.

- **Threema**

Dieser Anbieter erschien bis vor kurzem als echte Alternative zu WhatsApp sehr empfehlenswert und wird nach unserer Kenntnis auch von den Schweizer Behörden genutzt. Aber offenbar sind die Datenschutzeinstellungen nicht wirklich empfehlenswert. Z.B. schreibt https://www.chip.de/news/Sichere-WhatsApp-Alternative-Edward-Snowden-empfiehlt_135258856.html:
„Die Verschlüsselung ist allerdings nicht zweifelsfrei bekannt, da Threema anders als Signal kein Open-Source-Dienst ist."
Wir raten nicht unbedingt ab, können Threema aber auch nicht ausdrücklich empfehlen.

- **Telegram**

Dieser Messenger scheint als Alternative durchaus in Frage zu kommen, wird aber auch sehr unterschiedlich bewertet, was den Datenschutz anbelangt.
Hierzu schreibt https://www.chip.de/news/Sichere-WhatsApp-Alternative-Edward-Snowden-empfiehlt_135258856.html:
„Ähnlich wie …….. verschlüsselt Telegram seine Nachrichten mit Ende-zu-Ende-Verschlüsselung, sodass Eindringlinge und neugierige Mitleser ausgesperrt werden. Zwar ist der Dienst nicht komplett Open Source, hat dafür aber eine größere Nutzerschaft als Signal."
Wir raten nicht unbedingt ab, können Telegram aber auch nicht ausdrücklich empfehlen.

- **Signal**

Signal wird allseits zur Zeit als „die“ Alternative im Bereich der Messenger-Dienste angesehen und ist nicht nur aus unserer Sicht, sondern im März 2020 sogar von Edward Snowden zu empfehlen.

https://signal.org/de/
https://support.signal.org/hc/de

Aber auch der sehr kritische Kuketz-Blog soll hier zu Wort komen, Auszug aus:
http://www.kuketz-blog.de/empfehlungsecke

„Mir sind die Nachteile von Signal wohlbekannt (Telefonnummer-Upload, zentraler Dienst, Amazon-Server etc.). Ich habe Signal selbst mehrfach kritisiert – für den Durchschnittsanwender ist dieser Messenger nach meiner Auffassung allerdings die beste Wahl. Zumal bei der Nutzung kaum Meta-Daten anfallen und neue, innovative Technologien (Private Contact Discovery, Sealed Sender) zum Schutz der Privatsphäre umgesetzt werden. Die standardmäßig aktivierte Ende-zu-Ende-Verschlüsselung garantiert eine vertrauliche Kommunikation und wird regelmäßig auditiert. Gerade für Wechselwillige, die WhatsApp (endlich) hinter sich lassen möchten, ist Signal aufgrund der nahezu identischen Bedienbarkeit eine empfehlenswerte Alternative.“

Terminfindung:

Alternative zu Doodle:

https://nuudel.digitalcourage.de.

Und noch ein ganz allgemeiner Hinweis:

Fast alle der hier beschriebenen Angebote sind kostenlos, finanzieren sich dennoch nicht über versteckte Datenweitergabe oder individuell zugeschnittene Werbung. Es ist daher nur recht und billig, einen kleinen freiwilligen Beitrag zu leisten. Man findet eigentlich auf allen Seiten irgendwo die Möglichkeit zu spenden. Dass das meistens nicht sofort ins Auge springt, spricht nur noch mehr für die entsprechenden Anbieter.

Fragen, Ergänzungen, Rückmeldungen bitte an:

Klaus Grothe-Bortlik
Tel.: 089 / 53 29 56-15
klaus.grothe-bortlik@shz-muenchen.de