Schriftliche Zusammenfassung der Vor- und Nachteile zur Messengernutzung in einer Sozialen Beratungseinrichtung

Grundlage bildet die Ausarbeitung auf:
https://makeitsocial.net/messengervergleich-mit-schwerpunkt-auf-datenschutz-whatsapp-signal-threema-etc

Die Auswahl der hier analysierten Messenger basiert auf den derzeit meistgenutzten Diensten Whatsapp, Facebook Messenger, Telegram, Signal, Threema. Ergänzend dazu sind drei Produkte aus meiner persönlichen Empfehlung heraus eingeflossen.

Für die Nutzung eines Messengers für die Soziale Arbeit sind folgende Aspekte relevant:

1. Einhaltung der Vorgaben aus der DSGVO
2. Keine Auswertung oder Weitergabe von Meta-Daten (Verbindungs- und Nutzungsdaten)
3. Möglichst niedrigschwellig in der Anwendung (Installation, Kosten, Usability)

Wenden wir diese drei Parameter auf die Messenger in der Übersicht an, schließen sich die meisten bereits aus.

Whatsapp
Whatsapp gehört zu den meistgenutzten Messengerdiensten weltweit. Das ist auch gleichzeitig sein größter Mehrwert. Nahezu jede:r Nutzer:in kennt die Anwendung und nutzt sie mehr oder weniger regelmäßig. Seit 2014 gehört Whatsapp zum Facebook Konzern. Die Anwendung selbst ist mittlerweile kostenlos zu beziehen. Gleichzeitig handelt Facebook aber gewinnorientiert. Seit einigen Jahren hat Whatsapp das Verschlüsselungsprotokoll Axolotl (Signal-Protokol implementiert. Das Protokoll gilt als sicher, allerdings ist die Art und Weise wie die Ende-zu-Ende Verschlüsselung implementiert ist nicht öffentlich dokumentiert. Whatsapp betont immer wieder keine Inhaltsdaten auszuwerten, was durch das Axolotl-Protocol weitestgehend glaubhaft erscheint aber durch die eigene Implementation und fehlende Dokumentation auch nicht auszuschließen ist. Zudem wird dabei verschwiegen, dass Meta-Daten, also Verbindungs- oder Nutzungsdaten sehr wohl analysiert und die Erkenntnisse daraus innerhalb des eigenen Werbenetzwerkes weiterverarbeitet oder extern verkauft werden. Ende 2020 wurden Nutzer:innen dazu aufgefordert eine AGB Anpassung zu bestätigen, welche es Facebook zukünftig gestattet alle erhobenen Nutzungsdaten direkt im Werbenetzwerk des Konzerns zu verarbeiten. Spätestens seit dieser Ankündigung und der damit verbundenen medialen Aufmerksamkeit ist vielen Nutzer:innen dieses Vorgehen bewusst geworden. Dies hat zu einer massiven Abwanderung weg von Whatsapp, hin zu anderen Messengerdiensten geführt und gleichzeitig gezeigt, wie irrelevant die Datenschutzbedenken seiner Nutzer:innen dem Konzern sind.
Darüber hinaus stehen die Server in den USA und für die Anmeldung notwendige Voraussetzung ist das Übertragen des eigenen Telefonbuchs an den Anbieter. Da es keiner Zustimmung der im Telefonbuch der Nutzer:innen hinterlegten Kontakte bedarf und es sich bei der Telefonnummer um ein personenbezogenes Datum handelt, entspricht dieses Vorgehen einem klaren Verstoß gegen Artikel 4 der DSGVO.

Facebook Messenger
Siehe Whatsapp, außer Abgleich des Telefonbuchs.

Telegram
Telegram stellt derzeit für viele Menschen eine Alternative zu Whatsapp dar. Das ist verständlich, zumal sich die App in einem Funktionsumfang mit einigen sehr interessanten und praktischen Features präsentiert. Allerdings gibt es gute Gründe Telegram nicht zu nutzen.
Die App verwendet standardmäßig nur eine mittlerweile als grundlegend geltende Transportverschlüsselung. Die Chats sind standardmäßig unverschlüsselt und werden in der Servercloud des Anbieters auch so gespeichert. Das bedeutet, dass der Anbieter theoretisch ohne weiteres sämtliche Daten auswerten kann. Ob dies geschieht, dazu gibt es gegenwärtig keine Informationen. Die Verschlüsselung ist manuell aktivierbar, allerdings gilt dies lediglich für Einzelchats. Gruppen sind davon ausgenommen. Beim Verschlüsselungsprotokoll handelt es sich um MTProto. Dies ist eine Eigenentwicklung und grundsätzlich zunächst kein Problem. Leider ist lediglich die Client-App quelloffen (open-source) und die Serversoftware

unter Verschluss. Somit ist keine realistische Einschätzung über die Sicherheit und ggfs. vorhandene Hintertüren möglich.

Signal
Eine gute Alternative stellt Signal dar. Kostenlos, unkommerziell und von der „Signal Technology Foundation“, einer NGO mit dem Anspruch einen sicheren und zukunftsorientierten Messenger zu entwickeln, finanziert. Die gesamte Software ist open-source und es findet keine Speicherung von Daten in der Cloud statt. Die Kommunikation ist mit dem eigenen, quelloffenen Protokoll Axolotl, bzw. Signal-Protocol Ende-zu-Ende verschlüsselt. Zwar ist zur Anmeldung ebenfalls eine Telefonnummer notwendig und der Abgleich von Telefonkontakten wie bei Whatsapp ebenfalls erforderlich, allerdings werden lediglich „Hash-Werte“, also „verschlüsselte“ Zeichenketten statt der echten Nummern abgeglichen. Dadurch ist eine relative Anonymität gegeben und das Vorgehen entspricht den Vorgaben der DSGVO. Nach Angaben der Entwickler arbeitet man intensiv an einer Entkoppelung von Handynummer und Account.

Wire
Wire ist primär ein Business-Messenger. Das Geschäftsmodell der GmbH basiert auf Lizenzkosten zur Nutzung durch Unternehmen. Eine Auswertung von Meta-Daten ist nicht notwendig und wird nach gegenwärtigem Kenntnisstand auch nicht getan. Zwar ist eine Telefonnummer zur Nutzung notwendig, ein Abgleich der Kontakte ist aber nur optional. Zudem findet keine Speicherung von Chats und Medien in einer Cloud statt. Die Daten liegen verschlüsselt auf dem Smartphone und die Kommunikation ist mit dem Proteus-Protocol (eigene Implementation des Axolotl-Protocol) Ende-zu-Ende verschlüsselt. Leider ist die Serversoftware nur zu teilen einsehbar und läuft auf den Servern von Amazon Web Service in der EU.

Threema
Seit Ende 2016 veröffentlicht die Threema GmbH einen jährlichen Transparenzbericht, in dem sie Behördenanfragen offenlegt und die Art der in diesen Anfragen mitteilbare Daten erläutert. Threema wirtschaftet als GmbH gewinnorientiert, das Geschäftsmodell basiert hier allerdings auf der einmaligen Anschaffung der App für 2,99€. Eine Auswertung und Weitergabe von Meta-Daten ist dadurch nicht notwendig und wird nach gegenwärtigem Kenntnisstand auch nicht getan. Ein großer Vorteil von Threema ist, dass für die Nutzung keine Telefonnummer oder E-Mail notwendig ist und Firmensitz, sowie Serverstandort in der Schweiz liegt. Einzige Kritikpunkte sind, die Verschlüsselung mit dem NaCl-Protocol, welches es einem Angreifer in der Theorie ermöglicht durch einen abgefangenen Schlüssel auch zukünftige Nachrichten mitlesen zu können und das die Software nicht gänzlich als open-source veröffentlicht ist, aber sukzessiv wird.

Conversations
Conversations ist ein Messengerclient, der das quelloffenen Kommunikationsprotokoll XMPP nutzt. Es gibt drei verschiedene Verschlüsselungsprotokolle zur Auswahl und durch die freie Serverwahl (ähnlich einem E-Mail Anbieter) obliegt es den Nutzer:innen, welchem Anbieter sie am meisten vertrauen. Bei Bedarf kann auch ein eigener Server betrieben werden, sodass Datenschutzfragen ganz lokal beantwortet werden können. Die Weiterentwicklung wird von einem internationalen Zusammenschluss von freiwilligen Programmierern geleistet und zur Nutzung ist weder Telefonnummer, noch E-Mail oder ähnliches notwendig.

Caritas Beratungsplattform
Die Caritas setzt sich als großer Träger bereits länger mit den Möglichkeiten digitaler Beratungsangebote auseinander. Da kein am Markt verfügbarer Messenger den eigenen Ansprüchen an Benutzerfreundlichkeit, Datenschutz und Funktionsumfang gerecht und die Entwicklung einer eigenen App Zeit- und Geldverschwendung ist, hat man sich dazu entschlossen ein Chat-Portal zu entwickeln, welches auf allen Endgeräten mit gängigem Internet Browser gleich funktioniert.

Im Juni 2020 entschied man sich die Plattform nicht nur für die eigene Beratungstätigkeit zu nutzen, sondern allen Interessierten Einrichtungen als open-source Produkt zur Verfügung zu stellen. Da das Hosting selbst zu übernehmen ist, kann der Serverstandort selbstbestimmt werden. Lt. Caritas ist ein speichern von Meta-Daten nicht möglich. Die Aufbewahrungsfrist und Umfang für Serverlogs obliegt dem Hoster und kann selbst bestimmt werden. Für die Nutzung ist lediglich ein Benutzeraccount notwendig, der niedrigschwellig zu Beratungsbeginn festgelegt wird. Mithilfe eines Passworts kann der bisherige Verlauf wieder hergestellt werden und die Nutzung einer E-Mail Adresse optional.

Die Kommunikation mit dem Server ist SSL-Verschlüsselt und die Chatprotokolle werden ebenfalls verschlüsselt auf dem Server aufbewahrt.

Fazit
Abschließend ist festzustellen, dass nur wenige Messenger alle drei Voraussetzungen für eine bedenkenlose Nutzung in der Sozialen Beratung erfüllen.

Die Messenger Whatsapp und Facebook fallen gänzlich durch dieses Raster. Telegram wäre nach gegenwärtigem Kenntnisstand eine Option, sofern bei der Nutzung darauf geachtet würde die Verschlüsselung einzuschalten. Da die Ende-zu-Ende Verschlüsselung allerdings die Nutzung einer Desktop-Anwendung auf Seiten der Beratung verhindert, wäre für jede beratende Person ein eigenes Smartphone und die gesamte Beratung auch nur darüber möglich. Hinzu kommen die vielen Ungewissheiten, welche einer Nutzung im Weg stehen. Signal wäre grundlegend eine Option, dem entgegen steht allerdings der Serverstandort USA. Zwar entspricht das Vorgehen die Telefonnummer nur „gehashed“ zu übermitteln grundlegend der DSGVO, solange eine Entkoppelung von Account und Nummer aber nicht stattgefunden hat, würde ich von einem Einsatz im professionellen Umfeld zunächst abraten. Hinzu kommt, dass US-Amerikanische Unternehmen über den Patriots Act den Sicherheitsbehörden der USA gegenüber auskunftspflichtig sind und nicht sicher ist, welche Daten wann und zu welchem Zweck abgegriffen und genutzt werden.
Wire ist in jedem Fall ein Messenger der bedenkenlos eingesetzt werden kann. Allerdings kostet dieser für das ihn einsetzende Unternehmen 5€ / Monat pro Nutzer:in. Dies bezieht sich lediglich auf die professionelle Seite (Beratungseichrichtung) und sofern nicht unterschiedliche Telefonnummern für die Kommunikation zu den Adressat:innen zum Einsatz kommen sollen, kann ein Account auf 8 Geräte synchronisiert werden. Für Adressat:innen bleibt lediglich die Aufgabe der Installation und Einrichtung.
Gegen Threema spricht der Anschaffungspreis von 2,99€ was insbesondere in der Sozialen Beratung eine unüberwindbare Hürde darstellen könnte, welche Nutzer:innen davon abhält diesen Weg zu nutzen. Gleiches gilt für Conversations, hier 1,99€. Zwar ist die Nutzung von XMPP generell kostenfrei und andere Clients sogar kostenfrei verfügbar, allerdings wurde Conversations insbesondere für eine gute Usability entwickelt, welche den Anwender bei der Einrichtung unterstützt. Ohne den Einsatz von Conversations als Client-App wird die Einrichtung technisch nicht-versierte Menschen sicherlich vor Hürden stellen.
Die Beratungsplattform der Caritas bietet sich an, da sie speziell für die Soziale Beratung entwickelt wurde und auf allen Endgeräten niedrigschwellig mit einem Internet Browser einsetzbar ist. Da sie responsiv entwickelt wurde, funktioniert die Plattform auf einem PC gleichermaßen wie auf einem Smartphone und sämtliche Datenschutzbedenken obliegen dem Hoster. Einziger Nachteil ist, dass es zum Betrieb einen eigenen Webserver erfordert, welcher, sofern es eine Projektwebsite geben soll, sowieso vorhanden sein muss. Dagegen spricht lediglich, dass es eine Person geben muss, welche die Plattform aufsetzt und regelmäßig mit Updates versorgt, sowie den Webserver pflegt.
Ich schätze den Aufwand allerdings relativ überschaubar ein.

Philipp Fode | IT Services
Owiesenstraße 24
22177 Hamburg

Telefon: +49 40 60859490
E-Mail: itservices@fode-hh.de

www.fode-hh.de und www.makeITsocial.net

I ♥ IT | Philipp Fode IT SERVICES