

Isabel Zorn | Jule Murmann | Asmae Harrach-Lasfaghi

Datenschutzgerecht und barrierearm kommunizieren – Kriterien zur Auswahl von Messenger-Apps für Bildungseinrichtungen

Working Paper No. 6 im Rahmen des Projekts
IDiT – Including.Digital.Twins



GEFÖRDERT VOM

Impressum:

Autorinnen: Isabel Zorn, Jule Murmann, Asmae Harrach-Lasfaghi
Technische Hochschule Köln
Institut für Medienforschung und Medienpädagogik
Fakultät für Angewandte Sozialwissenschaften
Gustav-Heinemann-Ufer 54
D-50968 Köln

Kontakt:

Prof. Dr. Isabel Zorn

isabel.zorn@th-koeln.de

[Webseite: https://idit.online/](https://idit.online/)

Köln, April 2021

Zitiervorschlag:

Zorn, Isabel; Murmann, Jule; Harrach-Lasfaghi, Asmae (2021): Datenschutzgerecht und barrierearm kommunizieren. Kriterien zur Auswahl von Messenger-Apps für Bildungseinrichtungen. Hg. v. TH Köln. Köln (Working Papers IDiT, No. 6). Online verfügbar unter

https://idit.online/fileadmin/user_upload/Working_Paper/Messengerdienste_Kriterien_Bildungseinrichtungen_IDiT_WP6_Auf1.pdf

Quellenangaben des verwendeten Bildes auf der Titelseite: Hochschule Niederrhein – stock.adobe.com
Verwendung von Logos unter Markenrecht

Das dieser Veröffentlichung zugrunde liegende Vorhaben „IDiT – Including.Digital.Twins. Inklusives Mentoring und mediale Kompetenzen für RehabilitandInnen und Azubis in kaufmännischen Berufen/Berufsausbildung“ wurde im Rahmen der Förderrichtlinie „Inklusion durch digitale Medien in der beruflichen Bildung“ durch das Bundesministerium für Bildung und Forschung sowie den Europäischen Sozialfonds unter dem Förderkennzeichen 01PE18015B von 2018 bis 2021 gefördert. Es wurde von der TH Köln, der Hochschule Niederrhein und dem Berufsförderungswerk Köln (Leitung) durchgeführt.

Ziel der Europäischen Union ist es, dass alle Menschen eine berufliche Perspektive erhalten. Der Europäische Sozialfonds (ESF) verbessert die Beschäftigungschancen, unterstützt die Menschen durch Ausbildung und Qualifizierung und trägt zum Abbau von Benachteiligungen auf dem Arbeitsmarkt bei. Mehr zum ESF unter: www.esf.de.

Inhaltsverzeichnis

I Abstract	5
II English Summary	6
1 Einleitung	8
2 Digitale Kommunikation in Bildungseinrichtungen	10
2.1 Wachsende digitale Kommunikationsbedarfe in Bildungseinrichtungen	10
2.2 Risiken und Problematiken des Einsatzes von Messengern in schulischen oder sozialpädagogischen Kontexten	12
2.2.1 Datenschutz.....	12
2.2.2 Privatsphäre, Predictive Analytics und Exklusion	14
2.2.3 Medienkompetenz und Digitalkompetenz	15
3 Methode der Studie zur Auswahl von Messenger-Software in der beruflichen Bildung	18
3.1 Erhebung der Anforderungen für einen Messengereinsatz in Bildungseinrichtungen	18
3.2 Erstellung von Prüfkriterien	19
3.3 Auswahl der zu begutachtenden Messenger-Apps	20
3.4 Prüfung nach Datenschutzerfordernungen.....	22
3.5 Prüfung nach Features und Praktikabilität	23
4 Ergebnisse I: Besondere Anforderungen an Messenger-Kommunikation in Bildungseinrichtungen	23
4.1 Datenschutz/personenbezogene Daten	23
4.2 Schulrecht	24
4.3 Behördenkommunikation	25
4.4 Bildungsauftrag	26
4.5 Inklusion	26
4.6 Verpflichtung versus Freiwilligkeit der Nutzung.....	27
5 Ergebnisse II: Kriterien für die Auswahl von Software in Bildungseinrichtungen	27
5.1 Datenschutz, Privatsphäre	28
5.1.1 Grundlagen.....	28

5.1.2	Entwickelte Kriterien zum Umgang mit Datenschutz und Privatsphäre ...	30
5.1.3	Ergebnisse der Prüfung nach Datenschutz	32
5.1.3.1	DSGVO-Konformität von Messenger-Apps	32
5.1.3.2	Notwendigkeit des Abschlusses einer Vereinbarung zur Auftragsverarbeitung.....	35
5.2	Barrierefreiheit/-armut	37
5.2.1	Grundlagen	37
5.2.2	Kriterien der Prüfung auf Barrierefreiheit	40
5.2.3	Zusammenfassung der Prüfung auf Barrierefreiheit	41
5.3	Praktikabilität.....	42
5.3.1	Grundlagen.....	43
5.3.2	Kriterien der Prüfung.....	43
5.3.3	Ergebnisse der Prüfung auf Praktikabilität.....	46
6	Ergebnisse III: Potential von freien anbieterunabhängigen Messengern mit auftrags- oder eigengehosteten Chatservern	47
7	Auswahlentscheidungen für die Messenger-Dienste “Wire” und “Threema Work” für berufliche Bildung im Projekt IDiT	52
7.1	Einschlusskriterium: Individuelle Nutzbarkeit	52
7.2	Einschlusskriterium: Datenschutz	53
7.3	Von der engeren Auswahl zu Wire und Threema (Praxistest).....	55
7.4	Von Threema zu Threema Work.....	57
7.5	Zusammenfassung: Auswahlentscheidungen eines Messengers für die berufliche Bildung im Projekt IDiT.....	59
8	Zusammenfassung	60
III	Literaturverzeichnis.....	63
IV	Anhang: Websites der Messenger-Anbieter	68

I Abstract

Bildungseinrichtungen haben zunehmende Bedarfe für professionelle digitale Kommunikation. Bei der Auswahl geeigneter Kommunikationstools besteht Bedarf für geeignete Informationen als Entscheidungsgrundlage. Insbesondere Messenger-Kommunikation ist stark im privaten Alltag der Personen integriert. Während Bedarfe für umfangreiche datensichere Kommunikation in bildungsrelevanten Kontexten steigen, mangelt es an Konzepten für datengeschützte (Karaboga et al. 2014; Digitalcourage e.V. o.J.) und Privatsphäre wahrende Unterstützung von Bildungsprozessen durch Software, an verpflichtender Ausbildung für Fachkräfte (Zorn, Tillmann und Kaminski 2014; Imort und Niesyto 2014), sowie an verlässlicher Information für praktikable Software-Alternativen. Der Beitrag skizziert die besonderen Anforderungen von Bildungseinrichtungen bei der Auswahl geeigneter Software am Beispiel von Messenger-Kommunikation. Aus diesen Anforderungen werden Kriterien für benötigte Informationen als Entscheidungsgrundlage für die Softwareauswahl in drei Kategorien vorgestellt: Datenschutz/Privatsphäre, Barrierefreiheit/Barrierearmut, Praktikabilität.

Da bislang keine Kriterien und Good-Practice-Vorschläge vorlagen, wurde eine Studie zur Eruierung der Eigenschaften potenziell geeigneter Messenger-Software erstellt. Hierfür wurden zunächst notwendige Kriterien zu den drei genannten Kategorien definiert und im Anschluss deutsche und bekannte internationale Messenger auf die Datenschutz-Kriterien hin geprüft. Aufgrund der Ergebnisse zur Konformität mit der Datenschutz-Grundverordnung der EU (DSGVO) als Einschlusskriterium wurden die in Frage kommenden Messenger einem Praxistest unterzogen. Dabei wurden teilweise iterativ weitere praxisrelevante Kriterien der Praktikabilität entwickelt.

Neben institutionsinternen Messengern konnten unter den frei erhältlichen anbieterabhängigen Messengern sechs Dienste identifiziert werden, die zumindest bei Nutzenden über 16 Jahren DSGVO-konform genutzt werden können. Zum Zeitpunkt der Veröffentlichung sind dies nur noch fünf: Threema, Wire, SID, Ginlo,

Chiffry. Des Weiteren erscheinen anbieterunabhängige Messenger-Systeme, die den internationalen Standard für den Austausch von Chatnachrichten (XMPP) einhalten, als eine sinnvolle Möglichkeit für Bildungseinrichtungen. Hier kann ein eigenes oder beauftragtes Server-Hosting (im Verbund) möglich werden und es lässt sich bei einem IT-Dienstleister eine entsprechende Vereinbarung zur Auftragsdatenverarbeitung abschließen.

Für den Projektkontext IDiT – nämlich die berufliche Bildung für angehende Kaufleute für Büromanagement an Berufsschulen und an Berufsförderungswerken – werden die Entscheidungen für die Nutzung von „Wire“ und „Threema Work“ erläutert und begründet. Die zugrundeliegenden Überlegungen sind zwar auf den Projektkontext (Anwendung im Berufsförderungswerk Köln) zugeschnitten, aber verallgemeinerbar.

II English Summary

Educational institutions have increasing needs for professional digital communication. When selecting suitable communication tools, there is a need for appropriate information as a basis for decision-making. Messenger communication in particular is strongly integrated into people's private everyday lives. While needs for extensive data-secure communication in educational contexts are increasing, there is a lack of concepts for data-protected (Karaboga, Schütz, and Michael Friedewald, Peter Zoche, Tobias Matzner, Cornelia Mothes, Maxi Nebel, Carsten Ochs, and Hervais Simo Fhom 2014; Digitalcourage e. V. o.J.) and privacy-preserving support of educational processes through software, mandatory training for professionals (Zorn, Tillmann, and Kaminski 2014; Imort and Niesyto 2014), and reliable information for viable software alternatives. This paper outlines the specific requirements of educational institutions when selecting suitable software, using messenger communication as an example. From these requirements, criteria for

needed information are presented as a basis for software selection decisions in three categories: Data protection/privacy, accessibility/low-barrier, practicability.

Since no criteria and good practice suggestions were available so far, a study was conducted to elicit the characteristics of potentially suitable messenger software. To this end, the necessary criteria for the three categories mentioned were first defined and then German and well-known international messengers were tested for data protection criteria. Based on the results for conformity with the EU's General Data Protection Regulation (GDPR) as an inclusion criterion, the messengers in question were subjected to a practical test. In the process, additional practicality criteria were developed, in part iteratively.

In addition to institution-internal messengers, six services were identified among the freely available provider-dependent messengers that can be used in a GDPR-compliant manner, at least for users over the age of 16. At the time of publication, this leaves only five: Threema, Wire, SID, Ginlo, Chiffry. Furthermore, provider-independent messenger systems that adhere to the international standard protocol for the exchange of chat messages (XMPP) appear to be a viable option for educational institutions. In-house or commissioned server hosting would then be possible and a corresponding agreement for commissioned data processing can be concluded with an IT service provider.

The decisions to use "Wire" and "Threema Work" in the IDiT project context are explained and justified. The context was vocational training for prospective office management clerks at vocational schools and vocational training centers. Although the underlying considerations are tailored to the project context (application in the Berufsförderungswerk Köln), they can be generalized.

1 Einleitung

In einer zunehmend digitalisiert kommunizierenden Gesellschaft sind auch Bildungseinrichtungen herausgefordert, Entscheidungen darüber zu treffen, ob und wie sie mit ihren AdressatInnen digital kommunizieren. Wegen ihrer Verbreitung und häufigen Nutzung durch AdressatInnen und ihrer nützlichen Features kommen zunehmend auch ungeplant Messenger-Apps zum Einsatz, jedenfalls unter den AdressatInnen selbst. So kommunizieren zunehmend Schülerinnen und Schüler untereinander privat organisiert über WhatsApp über schulische Inhalte (Medienpädagogischer Forschungsverbund Südwest 2018). Landläufig zu beobachten ist zudem, dass immer wieder einzelne engagierte Mitarbeitende in Einrichtungen mit der Absicht der Verbesserung eines Prozesses mit KollegInnen oder AdressatInnen auf dem dienstlichen oder privaten Handy per WhatsApp kommunizieren und damit bewusst oder unbewusst Rechtsverstöße begehen. Derart privat organisierte Kommunikationskanäle zeigen den Bedarf auf, sind aber häufig nicht datenschützend. Entscheidungen der Einrichtungen darüber, ob und welche Software oder Apps (i.F. Software) sie nutzen, benötigen als Grundlage ausreichend gesicherte Informationen darüber, worauf bei der Auswahl zu achten ist. Bislang ist die Informationslage dünn. Zum einen liegen nicht ausreichend aussagekräftige und vergleichbare Daten über die einzelnen Softwares vor. Es existieren zwar diverse, teils auch detaillierte Kriterientabellen für freie Messenger-Apps (Wikipedia 2020; Verbraucherzentrale 2018; Williams o.J.; Digitalcourage e.V. o.J.; Cryptoparty 2019; Verbraucherzentrale 2020; Initiative Freie Messenger 2020b). Diese können aber meist nur für private Entscheidungen von Individuen als Information dienen, da für Organisationen der Bildung und Sozialen Arbeit umfassendere rechtliche Anforderungen und kontextspezifische Ziele bei der Nutzung bestehen.

Zum anderen benötigen Bildungseinrichtungen häufig systematisierte Anforderungskriterien. Wissenschaftliche Literatur zu den Anforderungen solcher Einrichtungen an interne und externe Kommunikation zur Erfüllung ihrer pädagogischen Aufgaben ist kaum existent: Welche Aufgaben sollen und müssen

durch Messenger-Kommunikation unterstützt werden? Welche Features können dafür störend oder hilfreich sein? Worauf ist bei der Inklusion aller möglichen Nutzenden zu achten? Welche Themen oder Kontexte erfordern oder verbieten die Nutzung von Messengern? Welche rechtlichen, ethischen und organisatorischen Konsequenzen kann die Messenger-Kommunikation nach sich ziehen? Wie ist die Akzeptanz von Messengern durch die AdressatInnen zu erwarten? Der beschriebene Mangel an Informationen begründet möglicherweise, warum bislang so wenige Einrichtungen systematisch Messenger einsetzen. Der Bedarf an geeigneten Informationen darf als hoch eingeschätzt werden, wenn Schulen und Jugendeinrichtungen hier bislang wenig bereitstellen und ihre Mitarbeitenden und AdressatInnen trotz Bedenken über Privatsphäre (vgl. mpfs 2018; D21 2017) „googeln“, „skypen“, „doodeln“ und „whatsappen“ und somit sensible Daten von teilweise schutzbedürftigen Menschen preisgeben. Wir haben bereits beschrieben, worauf beim Einsatz von Messengern in Kontexten der Sozialen Arbeit geachtet werden muss (Zorn, Murmann und Harrach-Lasfaghi 2021a). Der vorliegende Artikel zielt darauf, die Anforderungen von Bildungseinrichtungen an potenzielle Messenger-Kommunikation systematisch zu eruieren und somit einen Beitrag zur Informationsgrundlage zu leisten, ob und wie Privatsphäre wahrende Messenger-Software in Bildungskontexten zur Erreichung eines breiten schutzbedürftigen Bevölkerungsanteils eingesetzt werden kann.

Der Beitrag geht daher der Fragestellung nach:

Welche Kriterien bei der Auswahl einer Messenger-Software müssen und können Bildungseinrichtungen zugrunde legen?

Er erläutert zudem, warum diese Kriterien in Bildungseinrichtungen von Bedeutung sind. Die Ergebnisse werden kurz skizziert. Die Prüfungsergebnisse und Merkmalsausprägungen der einzelnen Messenger-Apps beschreibt die hier mehrfach zitierte Ergebnistabelle (Zorn, Murmann und Harrach-Lasfaghi 2021b).

2 Digitale Kommunikation in Bildungseinrichtungen

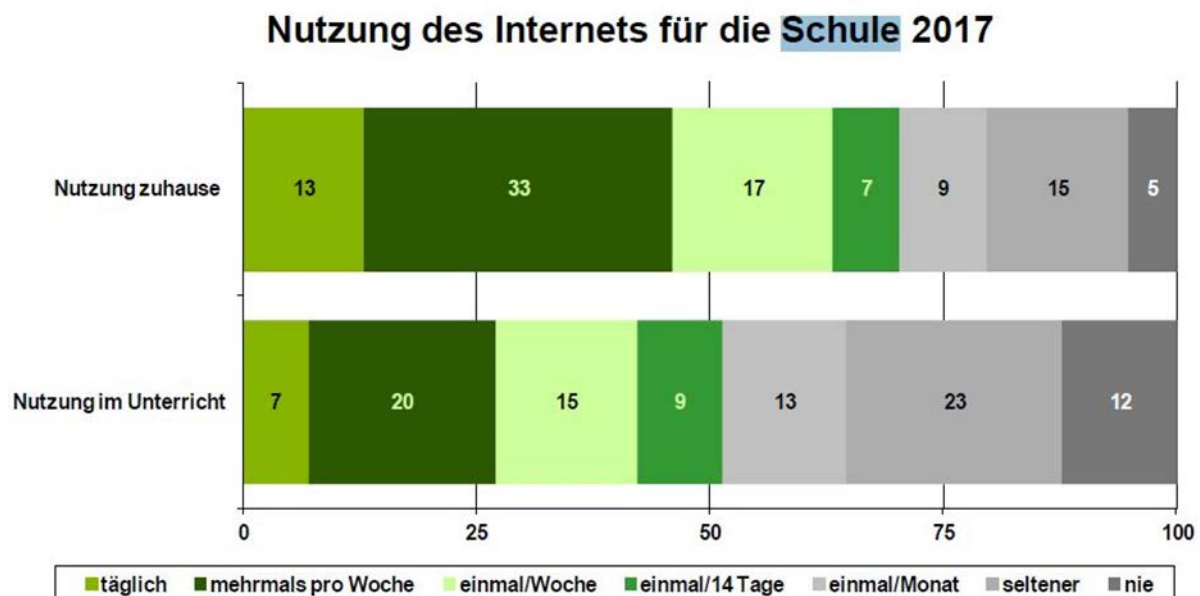
2.1 Wachsende digitale Kommunikationsbedarfe in Bildungseinrichtungen

Fast alle jugendlichen Schülerinnen und Schüler besitzen ein Smartphone (mpfs 2019). Die mobilen Kleincomputer können für die Kommunikation untereinander aber eventuell auch mit Lehrenden von großem Nutzen sein. Dazu zählen Schulorganisation, Informationsaustausch, kollaboratives Lernen per Messenger (vgl. Pöler 2018), aber auch informeller Austausch. Beispiele für Kommunikationsbedarfe, die sich mit Messengern umsetzen lassen, sind:

- Nachbesprechen von Aufgaben
- Gegenseitige Klärung von Fragen bei Hausaufgaben oder vor Klassenarbeiten
- Aufgabenübermittlung an fehlende, z.B. erkrankte Schülerinnen und Schüler
- Abfragen für Termine
- Erinnerungen an Zeiten und Treffpunkte oder Wegbeschreibungen bei Ausflügen
- Abfragen bei allen Eltern
- Absprachen unter den Lehrenden
- Aufgabenübermittlung und organisatorische Absprachen beim Distanzlernen
- Informeller Austausch

Man mag einwenden, dass all dies auch ohne Messenger möglich ist, doch über die Hälfte der Kinder und Jugendlichen geben an, dass sie sich ohne Smartphone die Schulorganisation nicht mehr vorstellen können, so das Ergebnis der JIM-Studien. WhatsApp, Youtube und GoogleDocs erfreuen sich zunehmender Nutzung durch Lernende (Medienpädagogischer Forschungsverbund Südwest 2017; Schmid et al.

2016). 87% der Jugendlichen nutzen eine WhatsApp-Gruppe für die Schulklasse (Medienpädagogischer Forschungsverbund Südwest 2020, 39)



Quelle: JIM 2017, Angaben in Prozent
Basis: alle Schüler, n=976

Abb. 1: Nutzung des Internets für die Schule

Lehrende an Berufsschulen nutzten laut einer Studie der Bertelsmann-Stiftung über die Digitalisierung der beruflichen Bildung (Schmid et al 2016: S. 27) nur zu 7% Messenger für den Berufsschulalltag, Ausbilder nutzen „Kommunikationsanwendungen, z.B. WhatsApp, Skype“ zu 18 % (a.a.O.: S. 32). Es zeigt sich danach, dass die Beteiligten eigene Lösungen zur digitalen Kommunikation suchen, wenn die Schulen oder ausbildenden Betriebe keine geeigneten Kommunikationsangebote zur Verfügung stellen. Diese Überlassung der Auswahl riskiert aber, dass die Auswahl der Tools möglicherweise nicht entlang von Regelungen bezüglich des Datenschutzes oder der Inklusion aller Schülerinnen und Schüler entschieden wird. Es ist zu vermuten, dass sich die populärsten Softwares ungeachtet ihrer schulbezogenen Eignung durchsetzen. Niedersachsen plant diesbezüglich im „Masterplan Digitalisierung“ ab 2021 das Smartphone als Lernmittel

einzusetzen. Datenschutzkonforme Alternativen zu WhatsApp, Dropbox, Google Drive etc. (vgl. Pöler 2018) fehlen aber weitgehend. Auch unter der sog. Corona-Krise zeigte sich der Bedarf an digital unterstütztem Unterricht mit sicheren E-Mail-Adressen, Messengern und Möglichkeiten des Datei-Austauschs. Für Jugendliche gilt schon seit geraumer Zeit, dass sie die Nutzung von WhatsApp unter Peer-Druck als „Pflicht“ verstehen (Gebel, Schubert und Wagner 2015). Erfahrungsgemäß kommt es häufig vor, dass sich in vielen Bildungseinrichtungen die Lernenden in ihren Klassen oder Studiengängen durch WhatsApp-Gruppen organisieren.

2.2 Risiken und Problematiken des Einsatzes von Messengern in schulischen oder sozialpädagogischen Kontexten

Um aufzuzeigen, worin die Problematiken liegen, wenn die gegebenen Bedarfe an digitalen Kommunikationstools von den Beteiligten durch eigene Lösungen befriedigt werden, werden im Folgenden Aspekte des Datenschutzes, der Privatsphäre, der Exklusion und der Medienkompetenz erläutert.

In Schulen und Bildungseinrichtungen wie den Berufsförderungswerken werden Menschen von großer Diversität ausgebildet, unter ihnen auch solche, die tendenziell zu eher benachteiligten, vulnerablen Gruppen gehören. Oft sind ihre finanzielle Situation, ihre Lebenssituation, ihre Teilhabemöglichkeiten unterdurchschnittlich und sie sind von weiteren Benachteiligungen bedroht. Daher sind die im Folgenden vorgestellten Problematiken wie Datenschutz und Barrierefreiheit praxisrelevante Kategorien für den Schutz und die aktuelle und zukünftige Chancengleichheit der Lernenden.

2.2.1 Datenschutz

Es werden bei allen oben beispielhaft genannten Softwareangeboten (WhatsApp, Youtube, GoogleDocs) personenbezogene Daten durch die Anbieter erhoben.

Personenbezogene Daten dürfen jedoch laut Datenschutzgrundverordnung (DSGVO) ausschließlich aufgrund bestimmter Rechtsgrundlagen oder mit wirksamen Einwilligungen der Betroffenen erhoben und ggf. verarbeitet und gespeichert werden. Für die im Rahmen des Erziehungsauftrages durch die Schulen erhobenen personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten sind eine solche Rechtsgrundlage u. a. die Schulgesetze. Diese regeln, dass personenbezogene Daten nur intern und nur für die geregelten Zwecke erhoben, gespeichert und verarbeitet werden dürfen. Die genannten Softwares geben die erhobenen Daten jedoch an Firmenserver weiter, wo sie gespeichert und verarbeitet werden. Der Datentransfer erfolgt oft unsichtbar im Hintergrund der App, wer keine genauen Kenntnisse hat, wird sie oft nicht bemerken und unbewusst Daten weitergeben. WhatsApp überträgt regelmäßig das gesamte Adressbuch eines Handynutzers an die Firmenserver in den USA. WhatsApp erhebt viele Informationen über die Nutzenden und ihre Geräte, einschließlich Geräte-ID und gleicht diese mit der Geräte-ID ab, die z.B. für Facebook genutzt wird (vgl. <https://www.whatsapp.com/legal/?l=de#privacy-policy>)

WhatsApp behält sich das Recht vor, die erhaltenen Daten auch an Facebook weiter zu geben, wo sie mit vielen Details über die Nutzenden verknüpfbar wären, z.B. Fotos, Vorlieben, Interessen, Verhalten, Likes. (vgl. <https://faq.whatsapp.com/general/security-and-privacy/how-we-work-with-the-facebook-companies?eea=1> , analytisch auch Pehl/Knödler 2020).

Wenn die App automatisch personenbezogene Daten der Kontaktpersonen versendet, muss eine Person, die WhatsApp auf dem Handy installiert, vorher alle Personen, deren Daten sie in ihrem Adressbuch gespeichert hat, um Erlaubnis bitten, diese Daten an WhatsApp weiterzuleiten. Das sog. WhatsApp-Urteil weist Erziehungsberechtigte auf ihre diesbezüglichen Fürsorgepflichten hin (Buchner 2017), eine Klage der Verbraucherzentrale läuft unter Aktenzeichen 52 O 22/17. Die Nutzung von WhatsApp für schulische Zwecke ist daher beispielsweise laut niedersächsischem Schulgesetz unzulässig (§ 31 NSchG) (Landesbeauftragte für den Datenschutz Niedersachsen 2018). In Schleswig-Holstein ist jegliche

Messenger-Nutzung in Schulen unzulässig. Es bestehen vielfältige ungeklärte schulrechtliche, organisatorische Fragen (LDB-SH 2016), u.a. zur Veraktung von Kommunikation der Lehrenden mit den Schülerinnen und Schülern und deren Eltern. Ein sehr guter Anhaltspunkt hierfür wären die bereits vorhandenen Regeln zum Umgang und zur Nutzung von E-Mail, da es eine Analogie zwischen „Chat“ und „E-Mail“ gibt (föderale Strukturen, selbe IT-Prinzipien). Ergänzend zu beachten sind lediglich typische Funktionen von Sofortnachrichten wie „Onlinestatus“, „tippt gerade“ und „zuletzt online“.

Weiterführende Links auf digitalen Angeboten der Bildungseinrichtungen, die auf externe Angebote verlinken, wie z.B. auf Erklärfilme bei YouTube, sind daher gegebenenfalls datenschutzrechtlich nur erlaubt, wenn die Lernenden vorher darüber informiert wurden und eingewilligt haben. Solche Links werden häufig auf Lernplattformen oder in Chats auf Messengern hinweisartig genutzt. Hier muss gegebenenfalls jedoch eine Einwilligung erfolgen.

Zum Schutz vor einer rechtlich bedenklichen Nutzung von Kommunikationstools reagieren viele Schulen mit Verboten, die jedoch nur schwer konsequent durchzuhalten sind. Zudem lösen sie das Problem nicht, da der Kommunikationsbedarf bestehen bleibt.

2.2.2 Privatsphäre, Predictive Analytics und Exklusion

Die derzeitigen und zukünftigen technischen Möglichkeiten der Erhebung und Verarbeitungen von scheinbar unwichtigen Daten lassen unerwartete Erkennungen, Rückschlüsse und Diagnosen von Personen zu. Die Analysen des Sprachassistentensystems „Alexa“ diagnostizieren akute Erkältungen oder Stimmungsschwankungen (Jin und Wang 2017). Schon seit einigen Jahren kann ein Algorithmus durch die Analyse geposteter Instagram-Fotos Depressionen diagnostizieren, und zwar treffsicherer als ausgebildete Psychologiefachleute in der Kontrollgruppe der Studie (Reece und Danforth 2017). Zukünftige erweiterte Analysemethoden für Verhaltensprognosen, z.B. über die Leistungsfähigkeit oder Krankheitsanfälligkeit, sind zu erwarten.

Daten von Lernenden können als besonders sensible Daten verstanden werden, wenn sie Rückschlüsse auf z.B. Fleiß, Durchhaltevermögen, Schnelligkeit, Peer-Netzwerke u.a. ermöglichen, miteinander verglichen oder mit anderen aussagekräftigen Daten verknüpft werden können. Insbesondere für benachteiligte Menschen aus vulnerablen Gruppen sind diese Diagnosen und Vorhersagen potenziell benachteiligend, wenn ihnen geringe Leistungsfähigkeit diagnostiziert oder vorhergesagt wird oder wenn zukünftig vermehrt solche Daten zum Verkauf stehen werden. Insbesondere Daten von schwachen Schülerinnen und Schülern, die sich in einem sensiblen Entwicklungsalter befinden, sind also zusätzlich aus diesen Gründen besonders schützenswert. Hinzu kommt, dass die Phänomene der digitalen Ungleichheit häufig auf diese Menschen zutreffen. So sind es häufig bildungsbenachteiligte Menschen, die im Zuge digitaler Ungleichheit (Bos et al. 2014; Klein und Pulver 2019; Iske und Kutscher 2020; Initiative D21 e.V. 2018, 24) auch weniger Kenntnisse im souveränen, datenschützenden Umgang mit digitalen Tools haben. Dies kann beispielsweise die Sicherung von Profilen und personenbezogenen Daten oder die Kontrolle von Cookie-Einstellungen und App-Berechtigungen u.v.m. betreffen. Es ist denkbar, dass die algorithmisch erstellten Vorhersagen über Menschen in Form von Daten und Profilen verkauft werden und beispielsweise bei Krankenkassen, Bewerbungsverfahren, Versicherungsleistungen entsprechend zu weiteren Benachteiligungen und geringeren Teilhabechancen führen können.

So kann das Bestreben, Menschen aktuell in pädagogischen Kontexten auch mittels digitaler Kommunikationstools zu inkludieren, ohne dabei deren Risiken zu berücksichtigen, dazu führen, dass Menschen zukünftig aufgrund der bei diesen Maßnahmen erhobenen Daten von Benachteiligungen oder Exklusionen bedroht sind.

2.2.3 Medienkompetenz und Digitalkompetenz

Solange ein Bedarf vorhanden und eine attraktive kostenlose, aber datenschutzrechtlich problematische Software diesen zu befriedigen verspricht,

dürften Verbote ohne die gleichzeitige Bereitstellung einer geeigneten Alternative nicht zielführend sein. Aufgabe und Herausforderung für Bildungseinrichtungen ist es zudem auch, die Medienkompetenz der Lernenden zu entwickeln und zu fördern, sie mit den Möglichkeiten und den Risiken sowie den Hintergründen des Umgangs mit digitalen Medien, und hier beispielsweise auch mit diversen und auch geeigneten Messenger-Angeboten, vertraut zu machen. Dafür ist Medienkompetenz und medienpädagogische Kompetenz bei den Fachkräften erforderlich. Die Vermittlung von medienpädagogischer Kompetenz in der Ausbildung in pädagogischen Studiengängen oder solchen für Soziale Arbeit ist jedoch marginal (Schulz und Sozialforschungsstelle TU Dortmund 2019; Imort und Niesyto 2014; Zorn, Tillmann und Kaminski 2014). Auch die Medienkompetenz in der erwachsenen Bevölkerung ist teilweise noch als gering zu bezeichnen (Initiative D21 e.V. 2018, 21ff). Ein Modell zur Entwicklung von medienpädagogischer Kompetenz für Fachkräfte liegt vor und führt aus, dass insbesondere die Identifizierung von geeigneten Medien im Handlungsfeld entsprechend aller zu berücksichtigenden Vorgaben zu leisten sein sollte (Siller, Tillmann und Zorn 2020).

Allerdings ist die Perspektive auf die Entwicklung einer medienpädagogischen Kompetenz bei Fachkräften nicht ausreichend: Selbst bei vorhandener Kompetenz ist die einer Entscheidung vorausgehende Recherche so aufwändig, dass sie einzelnen Fachkräften schlecht zugemutet werden kann. Die Recherchelage bezüglich der zu erfüllenden Vorgaben sowie der Erfüllung dieser Vorgaben durch diverse Software ist undurchsichtig, die Informationslage ist dünn. Die Recherchen innerhalb der von uns durchgeführten Studien zeigten eine große Unklarheit darüber auf, was LehrerInnen, SozialarbeiterInnen nutzen dürfen und sollen. Diese Unklarheit und die mangelnde Unterstützung beim Auswahlprozess können dazu führen, dass keine oder eine ungeeignete Nutzungsentscheidung getroffen wird. Die Komplexität eines Medienauswahlprozesses zeigte sich beispielhaft im Frühjahr 2020 unter COVID-19-Präventionsmaßnahmen, als selbst Hochschulen Unklarheiten bei der Auswahl DSGVO-konformer Kommunikationssoftware wg. teils unzureichender Angaben von Softwareherstellern, beispielsweise dem Videokonferenztool-Anbieter

Zoom erlebten. Wegen der dringenden Suche von sozialen Jugendeinrichtungen nach digitalen Kommunikationstools wurden Empfehlungen für Software in Jugendeinrichtungen gemacht, die eindeutig nicht DSGVO-konform sind (<https://www.jugendleiter-blog.de/corona/> und <https://www.offene-jugendarbeit.net/index.php/okja-in-corona-zeiten/okja-in-coronazeiten>).

So lässt sich erklären, warum trotz DSGVO und Landesschulgesetzen dennoch als kritisch einzustufende Software und Apps, beispielsweise WhatsApp, in Schulen und sozialen Einrichtungen zum Einsatz kommen (z.B. für Klassenchat, Streetwork, Wohngruppen).

Ein Verweis auf die Medienkompetenz unter Fachkräften als Erklärung greift demnach zu kurz (Zorn 2017).

Empfehlenswerte einführende Informationsportale zu sicherer Software allgemein existieren, z.B.

- Digitalcourage: <https://digitalcourage.de/digitale-selbstverteidigung>
- Klicksafe: <http://www.klicksafe.de>
- Me and my shadow: <https://myshadow.org/resources> (wird nicht mehr aktualisiert)
- Do not Track: <https://donottrack-doc.com/de/episodes>
- Internet-ABC: <https://www.internet-abc.de>
- Irights.info: <https://irights.info>

Außerdem existieren für die private Nutzung aussagekräftige Kriterienchecks für die Sicherheit von Messengern (Schönenberger 2016; Incobs 2015; Kuketz 2020; Williams o.J.; Wikipedia 2020; Neß o.J.; Initiative Freie Messenger 2020b).

Das Problem dieser bestehenden Informationsportale zu sicherer Software liegt jedoch darin, dass diese zwar Aussagen über individuelle sichere Nutzung machen, aber nicht aussagekräftig genug für Entscheidungen über den institutionalisierten Einsatz bieten.

3 Methode der Studie zur Auswahl von Messenger-Software in der beruflichen Bildung

Diverse Messengerangebote wurden nach Kriterien geprüft. Der Fokus der Studie lag darauf, Risiken und Möglichkeiten für einen Messengereinsatz in der beruflichen Bildung auszuloten und die dazu relevanten Kriterien zu entwickeln und systematisch darzustellen. Mögliche Apps wurden recherchiert, kategorisiert und theoretisch beurteilt. Für den Einsatz im Bildungskontext in Frage kommende Messenger-Apps wurden zudem praktisch erprobt. Im Anschluss sollte eine Entscheidung getroffen werden, ob und gegebenenfalls welcher Messenger im Projekt IDiT im Berufsförderungswerk und in anderen Kontexten beruflicher Bildung eingesetzt werden kann. Die Abwägungen dieses Auswahlprozesses aufgrund der entwickelten Kriterien werden im Kapitel 6 beschrieben

3.1 Erhebung der Anforderungen für einen Messengereinsatz in Bildungseinrichtungen

Die Erlaubnisse, Beschränkungen und zu berücksichtigenden Vorgaben für die Nutzung von Kommunikationssoftware in Bildungseinrichtungen sollten systematisiert erfasst werden. Dazu wurde umfangreich Literatur recherchiert, z.B. die Vorgaben durch Gesetze wie auch durch Landesdatenschutzbeauftragte. Zusätzlich wurden aufgrund der Aktualität und der bislang nur gering vorhandenen publizierten Forschung zur Thematik insbesondere internetbasierte Berichte, Kommentare sowie Fragen und Antworten an DatenschutzexpertInnen recherchiert. Aufgrund der geringen Verfügbarkeit aussagekräftiger gedruckter Literatur zur Thematik wurden ExpertInnen konsultiert in Form von ad-hoc Telefonaten/E-Mailanfragen (Datenschutzbeauftragte, Mitarbeitende Soziale Arbeit, LehrerInnen). Methodisch sollen hier nicht detaillierte Auswertungen der Befragungen vorgenommen werden. Die Anregungen der Befragten wurden als Ausgangsbasis für eigene Recherchen genutzt. Daraus erstellten wir eine systematische und begründete Darstellung der spezifischen Anforderungen von Bildungseinrichtungen.

Die Ergebnisse sind in Kapitel 4 dargestellt.

3.2 Erstellung von Prüfkriterien

Für eine informierte Analyse von Messengern und der Darstellung ihrer für Bildungseinrichtungen relevanten Eigenschaften mussten aus den dargestellten Anforderungen die rechtlichen und praktischen Grundlagen bestimmt werden sowie insbesondere daraus Kriterien entwickelt werden, nach denen man Messenger beschreiben, vergleichen und ihre Eignung für spezifische Kontexte bestimmen kann. Wir definierten die notwendigen Kriterien mithilfe der entwickelten Anforderungen basierend auf Erkenntnissen der Expertenbefragung, der Tabellenauswertung sowie der Literatur- und Gesetzesrecherche. Dazu wurden existierende Kriterientabellen zur Beurteilung von Messenger-Apps recherchiert (Wikipedia 2020; Verbraucherzentrale 2018; Williams o.J.; Digitalcourage e.V. o.J.; Cryptoparty 2019; Verbraucherzentrale 2020; Initiative Freie Messenger 2020b) und Kriterien für die Beurteilung der Barrierefreiheit von Apps im Allgemeinen herangezogen (Bundesministerium der Justiz und für Verbraucherschutz 2011; Oliveira 2016; Aktion Mensch und Stiftung Digitale Chancen 2010; Reh@pp-Quality 2016).

Wir prüften die dort verwendeten Kriterien und verglichen sie mit den Anforderungen an Bildungseinrichtungen. Im Ergebnis übernahmen wir Teile der dort genutzten Prüfkriterien. Es wurde dabei ersichtlich, dass die üblicherweise verwendeten Kriterien zwar ausreichen, um DSGVO-Konformität prüfen zu können, aber nicht ausreichen, um Barrierefreiheit und Praktikabilität zu prüfen. Zudem waren die Prüfkriterien teilweise sehr technisch formuliert, und es erfolgt durch uns eine Erläuterung ihrer Bedeutung und Relevanz für den Bildungskontext. Für die nicht ausreichenden Prüfungen entwickelten wir eigene Prüfkriterien für den Kontext inklusiver beruflicher Bildung und erläuterten diese.

Zusätzlich testeten wir jene individuell erhältlichen Messenger-Apps, welche die Datenschutzanforderungen nach eingehender Prüfung erfüllten. Anhand der Tests entdeckten und entwickelten wir weitere Prüfkriterien für die Praktikabilität einer App, weil erst durch das praktische Ausprobieren deutlich wurde, worin praktische Unterschiede einzelner Apps liegen können. Dies betraf beispielsweise notwendige Anforderungen oder Vorgehensweisen bei der Installation, bei der Integration von Kontakten, bei der Sicherung der Daten und anderes. Häufig fehlen solche Informationen bei den Herstellerangaben auf deren Webseiten, beispielsweise ist nicht immer angegeben, welche Daten notwendig sind bei der Inbetriebnahme der App (z.B. Telefonnummer? E-Mailadresse? SIM-Karte notwendig?). Das Modell der entwickelten Prüfkriterien wird in Kapitel 5 dargestellt.

3.3 Auswahl der zu begutachtenden Messenger-Apps

Nach der Entwicklung von Kriterien für Bedingungen der Einsatzmöglichkeiten von Messenger-Software sollte das Angebot der Vielzahl erhältlicher Messenger gesichtet und systematisiert werden.

Vorhandene Listen erhältlicher Messenger wurden gesichtet. Dabei wurde ersichtlich, dass die Listen unvollständig sind, z.B. fehlen Ginlo oder Quicksy auf der umfangreichen Wikipedia-Liste (Wikipedia 2020).

Aus dem Fundus der verfügbaren Messenger-Apps wurde eine Auswahl getroffen. Ausgewählt für die nähere Untersuchung wurden Apps/Messengersysteme,

1. die sehr populär und verbreitet sind und/oder
2. die deutsch oder europäisch basiert sind und eine Konformität mit DSGVO vermuten ließen.

Zu den ausgewählten Apps wurden umfangreiche Hintergrundinformationen recherchiert, teilweise führten wir Telefonate mit den Anbietern, um benötigte Informationen zu erhalten, weil sie nicht in frei verfügbaren Anbieterseiten oder

unabhängigen Kriterientabellen aufgeführt sind. Angaben auf letzteren überprüften wir wegen der Schnelllebigkeit der Entwicklungen auf den Anbieterseiten.

Die Recherchen ließen uns zu einer Systematisierung der Vielzahl an Messenger-Angeboten kommen:

Wir unterteilten Apps in 3 Gruppen:

A) für **Individuen**/Privatpersonen verfügbare **anbieterabhängige** (proprietäre) Messenger;

1.: Signal, WhatsApp, Telegram, Discord.

2.: Threema, Hoccer, Wire, SID, Chiffry, Ginlo.

B) für Individuen/Privatpersonen verfügbare anbieterunabhängige („freie“) und auf internationalem Standard (XMPP) basierte Apps¹;

für Android: Conversations, blabber.im (ehemals Pix-Art“), Quicksy.

für iOS: ZOM, ChatSecure, JabMe².

C) Von Unternehmen oder Institutionen erwerbbar Apps zur Bereitstellung für die institutionelle Kommunikation.

Das Angebot für institutionelle Lösungen ist groß. Unsere Auswahl war insofern beliebig, als der Fokus im Projekt IDiT zunächst nicht auf der Auswahl einer institutionellen App lag). Solche Apps sollten aber in die Untersuchung aufgenommen werden, um beispielhaft daran Möglichkeiten und Grenzen der Unternehmenslösungen aufzuzeigen: school.cloud, SchoolFox, OwnChat. Hierzu zählt zudem die später für das Projekt IDiT ausgewählte Unternehmenslösung Threema Work. Eine der dargestellten Apps sollte auf quelloffener Software

¹ Mit heutigem Kenntnisstand scheinen als „freie“ (anbieterunabhängige) Apps auch auf dem Protokoll Matrix basierende Apps vielversprechend, z.B. Element (Initiative Freie Messenger o.J.c).

² Mit heutigem Kenntnisstand scheint auch die Apps Siskin und Monal für iOS vielversprechend.

basieren, um die Möglichkeit des eigenen Hostings mit kostenloser Software aufzuzeigen: Mattermost.

Ziel der weiterführenden Prüfungen der Apps war, einen geeigneten, für Privatpersonen erhältlichen Messenger zu finden für die freiwillige Nutzung der Lernenden in beruflicher Bildung im inklusiven Projekt IDiT. Dies entsprang der Idee und dem Wunsch, mit der Auswahl und Nutzung einer Messenger-App im Bildungskontext gleichzeitig auch die Medienkompetenz und Messengerkompetenz der Lernenden in der Dimension ihrer Medienkunde zu erweitern und sie Erfahrungen machen zu lassen mit einer Messenger-App, die sie als DSGVO-konforme App auch im Privatleben nutzen könnten. Insofern fokussierten wir auf Apps, die nicht von der Bildungsorganisation als organisationsinterne App bereitgestellt werden müssen (vgl. Kapitel 7).

3.4 Prüfung nach Datenschutzerfordernungen

Die ausgewählten Messenger-Apps wurden im nächsten Schritt anhand der entwickelten Prüfkriterien zu Datenschutz analysiert. Ihre Merkmalsausprägungen zu den einzelnen Kriterien wurden recherchiert und in der Ergebnistabelle festgehalten. Um Informationen über ein Merkmal einer App zu erhalten, wurden zwar auch andere Vergleichsseiten (Wikipedia 2020; Verbraucherzentrale 2018; Williams o.J.; Digitalcourage e.V. o.J.; Cryptoparty 2019; Verbraucherzentrale 2020; Initiative Freie Messenger 2020b) rezipiert, um Anhaltspunkte für die Ausprägung bei einer App zu erhalten, jedoch wurden alle Merkmale auf den Anbieterseiten der App gesucht und belegt. Eine Problematik liegt darin, dass sich diese Eigenschaften einer App im Zuge schneller Entwicklungszyklen schnell ändern können. Insofern ist bedeutsam festzuhalten, dass die belegten Angaben für den Zeitraum Januar bis September 2020 gelten .

Die Ergebnisse finden sich tabellenartig in der publizierten Ergebnistabelle (<https://idit.online/publikationen>). Dort sind auch die die genutzten externen Vergleichstabellen in der Literaturliste aufgeführt.

3.5 Prüfung nach Features und Praktikabilität

Diese Prüfung erfolgte nach demselben Vorgehen wie die Prüfung zu Datenschutzanforderungen. Für das gesamte Sample wurden die Merkmalsausprägungen zu den entwickelten Kriterien der Praktikabilität recherchiert. Zudem wurden die DSGVO-konformen, individuell nutzbaren Apps auf diversen Geräten (unsystematisch) ausprobiert: sie wurden auf jeweils einem neueren und einem älteren iOS-Smartphone und Android-Smartphone installiert, in Betrieb genommen, ein Chatkonto angelegt, Kontakte wurden integriert und diverse Nachrichten und Medien untereinander versendet und Audio- und Videoanrufe unternommen. Die Erkenntnisse zu den vorhandenen Features und der Praktikabilität der Anwendungen wurden tabellarisch in Stichworten oder in Merkmalsausprägungen festgehalten.

4 Ergebnisse I: Besondere Anforderungen an Messenger-Kommunikation in Bildungseinrichtungen

Im Folgenden werden als Grundlage für die Entwicklung geeigneter Kriterien die besonderen Anforderungen in Bildungseinrichtungen skizziert. Diese Anforderungen sind die Grundlage für die zu entwickelnden Kriterien bei der Analyse von Messenger-Apps zu ihrer potenziellen Eignung für den Einsatz in Bildungseinrichtungen.

4.1 Datenschutz/personenbezogene Daten

In den Bundesländern liegen unterschiedliche Vorgaben vor, ob und wie Software in Bildungseinrichtungen verwendet werden dürfen. Bei kirchlichen Trägern wie dem BFW Köln kommen zudem noch spezielle kirchliche Datenschutzgesetze hinzu. Grundsätzlich ist – entsprechend der DSGVO – der Schutz von Daten mit Personenbezug zu beachten. Die Form des Schutzes kann aber unterschiedlich geregelt sein, beispielsweise ob grundsätzlich die Arbeit mit personenbezogenen

Daten auf bestimmte Geräte (nur Dienst-Computer, keine Smartphones) beschränkt ist.

Aus ihrem Auftrag ergibt sich, dass insbesondere die Berufsförderungswerke vorrangig mit vulnerablen Gruppen und daher mit besonders sensiblen Daten umgehen, denn schon die Zulassung zu beruflicher Ausbildung in einem Berufsförderungswerk ist an bestimmte Diagnosen oder Merkmale von Benachteiligung geknüpft. Bei der Erfüllung ihrer Aufgaben müssen die Einrichtungen daher beispielsweise die Vorgaben der Verbände und Träger beachten und sehen sich teilweise auch bestimmten ethischen Geboten, wie beispielsweise der Ethik des Berufsverbands DBSH (Deutscher Berufsverband für Soziale Arbeit e.V. 2014), verpflichtet.

4.2 Schulrecht

Für die Frage der Nutzung von Messenger-Diensten im schulischen und ausbildungsbezogenen Kontext gelten neben den üblichen Regelungen der Einhaltung telekommunikationsrechtlicher Vorschriften auch weitergehende schulrechtliche Fragestellungen. Dazu zählen Fragen zur inhaltlichen und rechtlichen Verbindlichkeit der Kommunikation oder dazu, ob die Kommunikation sicher ist und ob die dienstlichen Kommunikationsdaten sicher und technisch getrennt von privaten Kommunikationsdaten auf den privaten Endgeräten der Lehrkräfte verarbeitet (gespeichert) werden dürfen. Diesem Aspekt ließe sich aber begegnen durch die Nutzung von dienstlichen Geräten oder durch die Nutzung von Messenger-Diensten, die auch ohne Smartphone nur auf einem Computer funktionieren. Schulrechtlich relevante Praxisfragen sind: Wenn beispielsweise Lehrkräfte einer Schule systematisch Unterrichtsmaterialien oder Hausaufgaben ausschließlich über einen Messenger an die Schülerinnen und Schüler verteilen wollen: Kann die Schule voraussetzen, dass alle Schülerinnen und Schüler einer Klasse tatsächlich ein Endgerät (Smartphone, Tablet oder Computer) besitzen? Kann die Schule vorschreiben, dass ein Smartphone für die Gestaltung des Unterrichts vorhanden

sein muss und dafür genutzt wird? Ist es rechtlich möglich, einen bestimmten (ggf. kostenpflichtigen) Dienst vorzuschreiben? Unter welchen Bedingungen?

4.3 Behördenkommunikation

Schulen und Sozialarbeitseinrichtung müssen oft mit Behörden über rechtliche Aspekte ihrer Schützlinge kommunizieren. Insofern kann Kommunikation mit den Schützlingen rechtlich relevant werden. So stellen sich Fragen nach Möglichkeiten der Veraktung dieser Kommunikation – was bei E-Mail durch Ausdrucke leicht möglich ist, muss bei Messenger-Software geprüft werden. Ebenso ist zu klären, welche personenbezogenen Daten durch welche Stellen für welche Zwecke verarbeitet werden sollen und dürfen und ob mit dem Messenger empfangene oder versandte personenbezogene Informationen Aktenrelevanz haben könnten, dann kann in manchen Fällen eine Ende-zu-Ende-Verschlüsselung unerwünscht sein, weil Dritte (neben den zwei kommunizierenden Parteien) keine Einsicht nehmen können. In solchen Fällen muss eine normale Transportverschlüsselung der Daten ausreichen. Für die Brief- und E-Mail-Kommunikation gibt es in den Schulen in z.B. Schleswig-Holstein – wie wohl in allen öffentlichen Stellen in Deutschland – eindeutige Regelungen, welche Vorgänge in Schülerakten zu speichern sind. Öffentliche Stellen sind verpflichtet, die Rechtmäßigkeit ihres (Verwaltungs-)Handelns gegenüber der oder dem Betroffenen und ggf. gegenüber den Kontrollorganen wie z. B. Gerichten jederzeit nachzuweisen. Die Nachweispflicht im Zusammenhang mit personenbezogener Datenverarbeitung ergibt sich auch aus den Vorgaben der DSGVO und speziell im Schulbereich aus den Vorschriften des Schulgesetzes und der Schuldatenschutz-Verordnung. Ferner stellen sich Fragen zur Löschung der in einem Messenger gespeicherten Daten, die auf privaten Geräten der Lehrkräfte gespeichert sind. Für die Löschung der personenbezogenen Daten der Schülerinnen, Schüler und Eltern existieren in Schleswig-Holstein Vorschriften im Schulgesetz und der Schul-Datenschutzverordnung. Ferner hat das Bildungsministerium Dienstanweisungen für den Umgang mit E-Mails und deren Löschung getroffen.

Bei Kommunikation im Kontext Schule und Sozialarbeit ist zu beachten, ob Geheimhaltungspflichten anzuwenden sind und ob Sozialdaten übermittelt werden. Gesetzliche Vorgaben zu Geheimhaltung, strafrechtlicher Schweigepflicht und Sozialdatenschutz in der Sozialen Arbeit müssen eingehalten werden, dies ist insb. in § 203 Abs. 3, 4 Satz 2 Nr. 1 StGB sowie in Bestimmungen des § 80 SGB X geregelt. Es besteht eine Verschwiegenheitspflicht für die im professionellen Kontext geteilten Inhalte.

4.4 Bildungsauftrag

Bildungseinrichtungen haben einen Kernauftrag der Bildungsvermittlung. Dieser Bildungsauftrag umfasst unter den Bedingungen von Digitalisierung in der Gesellschaft und Veränderung der Lebenswelten auch die Vermittlung von Medienkompetenz und somit die Auseinandersetzung mit sicherer digitaler Kommunikation. Bieten diese Bildungseinrichtungen für Messenger-Kommunikation – die laut JIM-Studie 2020 zur aktivsten Internetbeschäftigung von 93% aller Jugendlichen zählt (Medienpädagogischer Forschungsverbund Südwest 2020) – keine Bildung und Angebote zur sicheren Nutzung, so übergehen sie nicht nur Kommunikationsbedarfe, sondern auch ihren Bildungsauftrag: Wo sollen Jugendliche und Menschen in beruflicher Ausbildung Kompetenzen in diesen bedeutsamen Bereichen erwerben, wenn nicht in ihren Bildungseinrichtungen?

4.5 Inklusion

Zudem haben Einrichtungen der Bildung Inklusion als Pflicht und Auftrag, hier ist insbesondere die UN-Behindertenrechtskonvention mit den Art. 9, 21, 22, 24 zu nennen, die sich auf Zugänglichkeit zu allen Informationen und IKT-Technologien sowie zu Bildung beziehen, um gleichberechtigte Teilhabe an allen gesellschaftlichen Prozessen zu ermöglichen. Insofern muss bei der Auswahl einer Messenger-Software die Zugänglichkeit und Barrierefreiheit beachtet werden, um niemanden strukturell von Informationsprozessen zu exkludieren. Kenntnisse sowie

Geräteausstattungen der Lernenden können dabei deutlich heterogen sein. Es werden unterschiedliche Betriebssysteme, teilweise in alten Versionen verwendet. Bedienungs- und Nutzungskennnisse variieren stark, es ist teilweise auf Lese- und Rechtschreibschwäche oder sogar Analphabetismus zu achten. Auch das Alter der Nutzenden ist heterogen, in Schulen liegt es meist unter 16 Jahren, in berufsbildenden Einrichtungen kann jedoch meist von einem Alter über 16 Jahren ausgegangen werden. Das Mindestalter von 16 Jahren ermöglicht die selbständige Entscheidung zu bestimmten Einwilligungen bei der Nutzung von Apps.

4.6 Verpflichtung versus Freiwilligkeit der Nutzung

Wo die entsprechenden rechtlichen Grundlagen (z.B. Schulrecht) geschaffen wurden (Nebel 2021, 21.22.2019), kann eine Verpflichtung zur Nutzung digitaler Werkzeuge in der beruflichen Bildung ermöglicht werden. Wenn diese nicht vorliegen, gilt die Freiwilligkeit:

Die Nutzung digitaler Zusatzangebote, welche nicht zum notwendigen Regelangebot der Bildungseinrichtung gehören, muss freiwillig und ohne Androhung von Nachteilen erfolgen können. Prüfungsrelevante Inhalte dürfen nicht ausschließlich über solche Dienste vermittelt werden. Unter welchen Bedingungen in der Schule die Nutzung eines Endgeräts (Smartphone, Tablet oder Computer) und eines bestimmten Messengers verpflichtend gemacht werden kann, ist eine noch ungeklärte schulrechtliche Frage (siehe 3.2). Das Einholen von Einwilligungen ist aus juristischer Sicht zu vermeiden (Nebel 21.22.2019). Bei anbieterunabhängigen Messengersystemen kann den NutzerInnen freigestellt werden, welches Programm / welche App diese für sich verwenden wollen.

5 Ergebnisse II: Kriterien für die Auswahl von Software in Bildungseinrichtungen

Den o.g. relevanten Anforderungen muss eine neu einzusetzende Software entsprechen, um in Bildungseinrichtungen einsetzbar zu sein. Dazu müssen zu den

Anforderungen die rechtlichen und praktischen Grundlagen bestimmt werden, die für die Planung eines Software-Einsatzes relevant sind. Auf diesen Grundlagen wurden im nächsten Schritt Kriterien entwickelt, nach denen Software – hier einzelne Messenger-Apps – geprüft werden kann.

Zusammengefasst müssen Kriterien für die Messenger-Auswahl für drei Kategorien entwickelt werden:

- a) Datenschutz und Privatsphäre;
- b) Barrierefreiheit und Inklusion;
- c) Praktikabilität des Einsatzes in Institutionen.

5.1 Datenschutz, Privatsphäre

5.1.1 Grundlagen

Grundlagen für die Kriterienentwicklung sind:

- (1) Datenschutzgrundverordnung (DSGVO)
- (2) Schulrecht
- (3) Gesetzliche Vorgaben zu Geheimhaltung, strafrechtlicher Schweigepflicht und Sozialdatenschutz

Zu 1: Die Erfüllung der Richtlinien der Datenschutzgrundverordnung (Europäisches Parlament 2016) ist Grundvoraussetzung für die Auswahl einer Software in allen institutionellen Einrichtungen (während Privatpersonen sich entscheiden können, ihr Recht auf Privatsphäre nicht wahrzunehmen). Dabei helfen konventionelle Prüftabellen, um Ausschlüsse von Messengern bei der Auswahl vornehmen zu können.

Die DSGVO bestimmt, wie personenbezogene Daten verarbeitet werden dürfen, indem sie Grundsätze (Art. 5 DSGVO) und Rechtmäßigkeiten (Art. 6 DSGVO) der Verarbeitung personenbezogener Daten regelt. Dazu zählt beispielsweise, ob die Verarbeitung der eigenen Telefonnummer und E-Mail-Adresse eine Einwilligung erfordert. Wenn sie eine Einwilligung erfordert, ist eine App-Nutzung in Deutschland

erst ab 16 Jahren zugelassen oder die elterliche Einwilligung ist erforderlich (Art.8 DSGVO).

Ein wesentliches Kriterium für DSGVO-Konformität ist die Frage, ob und welche personenbezogenen Daten erhoben und weiterverarbeitet werden. Besonders sensibel ist daher die Frage, wie eine Software mit Kontaktdaten aus Adressbüchern von Smartphones verfährt und ob diese Kontaktdaten vom Anbieter der Software gespeichert und verarbeitet werden.

Zu 2: Das Schulrecht regelt in jedem Bundesland die Rechte und Pflichten und die Ziele, die dem Lernen und Lehren in dem Bundesland zugrunde liegen. Dazu gehört unter anderem, wie geregelt ist, welche Medien und Lehrmaterialien und welche Lehr- und Lernsysteme in Schulen eingesetzt werden können (z.B. § 1 Abs. 6 SchulG RLP). In dem Zuge ist auch geregelt, ob eine Neueinführung einer digitalen Kommunikations- und Lernform (beispielsweise über einen Messenger) möglich ist und ob die Nutzung zwingend oder nur freiwillig erfolgen kann und wie mit der Übermittlung von Daten an Dritte zu verfahren ist (z.B. § 67 Abs. 6 SchulG RLP). Im Schulgesetz ist zudem geregelt, welche Daten Mitarbeitende wie LehrerInnen oder Schulsozialarbeitende erheben, speichern oder teilen oder an Dritte weiterreichen dürfen (für eine Übersicht als Handreichung für LehrerInnen vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin 2005). Da beim Einsatz einer Messenger-App potenziell Namen und Kontakte sowie Inhalte geteilt werden, sind die schulrechtlichen Voraussetzungen in einen Zusammenhang mit den technischen Möglichkeiten einer Messenger-App zu stellen.

Prüfkriterien können sein: Ist Übernahme in eine Akte möglich? Ist Computernutzung möglich? Ist Nutzung notwendig oder freiwillig?

Zu 3: Gesetzliche Vorgaben zu Geheimhaltung, strafrechtlicher Schweigepflicht und Sozialdatenschutz in der Sozialen Arbeit, die auch z.B. für die Schulsozialarbeit gilt, müssen eingehalten werden, dies ist insb. in § 203 Abs. 3, 4 Satz 2 Nr. 1 StGB sowie in Bestimmungen des § 80 SGB X geregelt. Es besteht eine Verschwiegenheitspflicht für die im professionellen Kontext geteilten Inhalte.

5.1.2 Entwickelte Kriterien zum Umgang mit Datenschutz und Privatsphäre

Entsprechend der Anforderungen an Bildungseinrichtungen entwickelten wir die folgenden Prüfkriterien. Dazu wurden die im Methodenkapitel genannten allgemeinen Vergleichstabellen genutzt, deren Kriterien wir entsprechend der o.g. Anforderungen übernahmen und ergänzten. Dieser Prozess erforderte teilweise eine Bewertung technischer Eigenschaften sowie ihrer praktischen Relevanz in Bildungskontexten. (Welche Relevanz hat es für den Datenschutz in einer Bildungseinrichtung, ob ein Messenger quelloffen und somit überprüfbar ist, ob er kostenpflichtig ist, wie viele Metadaten anfallen, ob der Server in der EU oder in Deutschland steht, ob das Adressbuch versendet wird, ob alle Kommunikation oder nur Teile davon Ende-zu-Ende verschlüsselt sind?)

Im Ergebnis entwickelten wir für die Prüfung des Schutzes der übermittelten Daten in Bildungseinrichtungen die folgenden Prüfkriterien für Messenger-Apps:

1. Gesamteindruck nach der Europäische Datenschutz-Grundverordnung: Konform nach Art. 5 und 6 DSGVO?
2. Standort des Dienstes
3. Infrastruktur des Dienstes
4. Einwilligung: Altersfreigabe (Art. 8 DSGVO): Messenger-Apps, die zur Registrierung die Preisgabe personenbezogener Daten erfordern, unterliegen nach Art. 8 DSGVO einer Altersbeschränkung von 16 Jahren. Ansonsten ist die Einwilligung eines Erziehungsberechtigten notwendig.
5. Anmeldung und Inbetriebnahme: Sind personenbezogene Daten also z.B. Telefonnummer, E-Mail, echter Name etc. für die Anmeldung notwendig?
6. Werden Nutzerdaten und/oder Meta-Daten gespeichert? (Prinzip der Datensparsamkeit) (Metadaten: Wer wann online ist; mit wie vielen und welchen Geräten jemand online ist; welche Kontakte jemand hat. Aus Metadaten lassen sich sehr viele Rückschlüsse über eine Person ableiten,

z.B.: Wer mit wem wann kommuniziert (oder auch nicht kommuniziert); wer an welchen Gruppen teilnimmt.

7. IP-Adressen der Geräte
8. Store and Forward: Teilstreckenverfahren der Datenübertragung, bei der Informationen über eine Zwischenstation (z. B. einen Router) gesendet werden, welche die Daten speichert und zu einem späteren Zeitpunkt an das finale Ziel oder eine weitere Zwischenstation weiterleitet.
9. Datentransfer: Schützt die App meine Nachrichten und Anhänge?
10. Prinzip der Zugänglichkeit und Offenheit: Ist die Datenschutzerklärung auf Deutsch verfügbar?
11. Adressbuch: Was geschieht mit Kontakten aus dem Adressbuch? Werden die Kontaktdaten auf den Server des Anbieters hochgeladen und dort lesbar gespeichert und verarbeitet?
12. Ende-zu-Ende Verschlüsselung: Eine lesbare Information (Klartext) wird durch einen Schlüssel in einen ohne diesen Schlüssel nicht lesbaren Text umgewandelt. So wird sichergestellt, dass die Entschlüsselung nur auf den Endgeräten der beteiligten Nutzenden (und nicht auf dem Transportweg der Nachricht und nicht auf dem Server des Anbieters) erfolgen kann.
13. Verschlüsselung & Datensicherheit: Welche kryptographische Methode wird angewendet?
14. Prinzip der Offenheit: Bietet das Unternehmen einen Transparenzbericht?
15. Revisionsfähigkeit: Es kann rückwirkend festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
16. DSGVO-Siegel: Dieses Siegel hat nur einen Vermarktungswert, kann aber für wenig versierte Nutzende eine Entscheidungshilfe darstellen.
17. Standort-Tracking: Sendet die App den eigenen Standort? Standortdaten sind nach Art. 4 Nr. 1 s. 1 DSGVO personenbezogenen Daten. Nach Art. 5 DSGVO gilt das Prinzip der Datenminimierung. Erfassung und Verarbeitung von Standortdaten dürfen nur mit einer Einwilligung erfolgen.

18. Quelloffenheit („Open Source“): Ist der Quellcode offen? Nur bei offengelegtem Quellcode sind Teile der Datenschutzangaben des Anbieters überprüfbar.

5.1.3 Ergebnisse der Prüfung nach Datenschutz

5.1.3.1 DSGVO-Konformität von Messenger-Apps

Die Kriterien wurden die Merkmale der Messenger-Apps der Gruppen A, B, C recherchiert. Aus der Gruppe der individuell nutzbaren anbieterabhängigen Messenger-Apps (Gruppe A) sind meisten populären, verbreiteten Apps problematisch in Bezug auf ihre unverschlüsselte Übertragung und Verarbeitung der Kontakte aus dem Adressbuch (die eigentlich eine Erlaubnis der Kontaktpersonen benötigt), ihren Serverstandort, und der Erhebung und Nicht-Verschlüsselung von Metadaten. Mit Ausnahme von Telegram bieten alle Apps standardmäßig eine Ende-zu-Ende-Verschlüsselung der Nachrichteninhalte an.

Die folgenden für Individuen verfügbaren anbieterabhängigen Messenger-Apps (Gruppe A) können nach der Anwendung der Prüfkriterien als DSGVO-konform gelten:

- Threema (nur teilweise quelloffen)
- Hoccer (existiert aktuell nicht mehr)
- Wire
- SID (nur Beta-Version verfügbar; Details und Informationen zum Protokoll und verwendeten Standards, der Verschlüsselung und dem Quellcode lediglich angekündigt wird; die Downloadadresse der Android-App läuft (Stand 02/2021) ins Leere)
- Ginlo
- Chiffry

Zur Einschätzung der prinzipiellen Nutzbarkeit von Threema in der Sozialen Arbeit nach DSGVO-Konformität kommt auch eine aktuelle explizite juristische Betrachtung (Pehl und Knödler 2020).

Darüber hinaus gibt es auch noch die Möglichkeit von anbieterunabhängigen Apps, die den internationalen Standard „XMPP“ einhalten (Gruppe B). Eine Messenger-App oder ein Programm, das dieses Protokoll („XMPP“) spricht, ist – anders als proprietäre Messenger-Apps – nicht an einen zentralen Serveranbieter gebunden. Deshalb werden solche Apps als „freie“ Messenger oder anbieterunabhängige Messenger bezeichnet. Mit diesen können die Dienste diverser Serveranbieter in Anspruch genommen werden oder es ist auch ein Auftrags- oder Eigenhosting möglich. Ob Serverbetreiber DSGVO-konform mit der Erhebung, Verarbeitung und Speicherung der Daten und Metadaten umgehen, kann also nicht auf die App selbst zurückgeführt werden. Insofern können mit diesen Messengern sowohl DSGVO-konforme als auch nicht DSGVO-konforme Serverbetreiber genutzt werden. Eine Prüfung der Kriterien kann nicht nur anhand der verwendeten App erfolgen, sondern hängt (wie bei E-Mail auch) vom Serverbetreiber ab. Es muss einen Vertrag zur Auftragsdatenverarbeitung mit diesem geben. Das Potenzial dafür ist aber aufgrund der Apps vorhanden: Adressbucheinträge werden nicht automatisch weitergeleitet, auf Mobilgeräten funktionieren die Apps auch ohne Zustimmung zum Zugriff auf das Adressbuch. Fast alle Apps sind ohne Angabe von Telefonnummer oder E-Mail-Adresse nutzbar (Ausnahme: Android-App „Quicksy“, das eine Sonderversion von Conversations für einen schnellen Einstieg unter Android ist).

Alle Messenger, die Adressbucheinträge unverschlüsselt weiterleiten und auf Servern speichern, sind nicht DSGVO-konform, wenn davon auszugehen ist, dass die Kontakte nicht danach gefragt wurden, ob sie mit einer Weitergabe ihrer Daten an Dritte (z.B. Firmen und Server) einverstanden sind. Dazu zählen je nach Betriebssystem auch verbreitete Apps wie WhatsApp, Telegram, Facebook Messenger, Skype, Viber, Discord, u.v.a.m.

Damit wird deutlich: Die weit verbreiteten Messenger erfüllen nicht die Grundvoraussetzung der Nutzung. Insofern gilt die Notwendigkeit, für den in Frage

stehenden Nutzungskontext eine Messenger-Software auswählen zu müssen, die nicht weit verbreitet ist. Eigentlich müsste das Messenger-System gewählt werden, das dann mit einem oder mehreren Messenger-Klienten (App/PC-Programm) genutzt werden kann. Damit wird jedoch ein bislang starkes Argument für die Nutzung von Messengern geschwächt, nämlich ein Medium zu nutzen, welches Lernende ohnehin im Alltag nutzen und auf ihrem Gerät bereits installiert haben.

„Institutionsinterne“ Messenger (Gruppe C) zählen zu den die DSGVO potenziell eingehenden Messengern. Hier wird ohnehin von der Bildungseinrichtung ein Vertrag mit dem Softwareanbieter abgeschlossen. Darin kann eine Vereinbarung zur Auftragsdatenverarbeitung den entsprechenden Schutz der Daten vertraglich absichern. Dazu zählen beispielsweise die „Enterprise-Versionen“ von Threema, Wire, Chiffry, SchoolCloud, OwnChat, Mattermost, Microsoft Teams und andere. Allerdings bleiben leider weiterhin teilweise Fragen zum Datenschutz offen und ein Austausch mit organisationsfremden Kontakten (Elternvertretungen, Eltern, Behörden, anderen Schulen, FreundInnen, ...) ist mit einem geschlossenen System, kaum möglich. Das wiederum schränkt die Nutzung im Gegensatz zu E-Mail (förderiertes System) ein.

Die häufig auch als sehr datensicher eingeschätzte und mittlerweile recht verbreitete App Signal wurde u.a. von der US-amerikanischen Regierung mitfinanziert ([https://de.wikipedia.org/wiki/Signal_\(Messenger\)](https://de.wikipedia.org/wiki/Signal_(Messenger))) und die Server stehen in USA, nicht in der EU. Dies kann als Ausschlusskriterium gewertet werden, weil Signal dadurch nicht der Anwendbarkeit der DSGVO unterstellt ist. Da Signal aber den Schutz entsprechend DSGVO sicherstellen will, hat es sich zwar der nicht einklagbaren Selbstverpflichtung mithilfe des Privacy Shields unterworfen. Kritik daran ist die mangelnde Einklagbarkeit und dass der Zugriff durch ausländische Geheimdienste nicht geregelt ist, zudem wurde die Eignung des Privacy Shields durch ein europäisches Gerichtsurteil im Jahr 2020 gekippt.

Somit wird deutlich, dass die Auswahl an Messengern begrenzt ist, für die die DSGVO Anwendung findet und die entsprechend mit personenbezogenen Daten umgehen.

5.1.3.2 Notwendigkeit des Abschlusses einer Vereinbarung zur Auftragsverarbeitung

Wenn über einen Messenger im Kontext einer Kommunikation in einer Bildungseinrichtung Daten anfallen, die unter die Geheimhaltungs- oder Verschwiegenheitspflicht fallen, ist zu prüfen, ob der Messenger-Anbieter die Verschwiegenheit übernimmt und sicherstellen kann. Rechtlich kann dies aber eine Grauzone sein. Beispielsweise fallen bei allen Messenger-Anbietern auch Metadaten an (z.B. wer hat wann mit wem wie lange kommuniziert), die durchaus aussagekräftig sind. Die Dauer der Speicherung und die Menge der gespeicherten Metadaten hat Relevanz. Rechtssicherheit kann nur durch Abschluss einer Vereinbarung zur Auftragsverarbeitung nach § 28 DSGVO erzielt werden. Ein Kriterium ist also, ob eine solche mit dem Anbieter des Produkts abschließbar ist. Das ist selbst bei anbieterunabhängigem Chat möglich. Hier gibt es gewerbliche Unternehmen oder eingetragene Vereine, die entsprechende Server betreiben und das sicherstellen. Der Allgemeinheit zur Verfügung gestellte Server von Privatpersonen können dieses Kriterium nicht erfüllen. Praktisch und sicher kann dies auch durch einen Vertragsabschluss bei einer Bezahlvariante eines Messengers möglich werden, beispielsweise also für Enterprise-/Pro-Versionen von Messengersystemen, also organisationsinternen Lösungen. Meist sind sogar Consumer- und Work-Versionen einer Messenger-App kompatibel und die Notwendigkeit des Kaufs einer Pro-Version nur für die professionellen Fachkräfte erforderlich (ausführlich zu allen rechtlichen Prüfungen: Pehl/Knödler 2020). Die Möglichkeiten einer Auftragsverarbeitungsvereinbarung sind für eine Einrichtung rechtssicher und somit vorteilhaft, da sie eine gegebenenfalls notwendige Einwilligung nach Art. 6 oder 8 DSGVO der Nutzenden überflüssig machen, die

immer Schwierigkeiten (Rücknahme der Einwilligung, Einwilligungen bei Machtgefällen) mit sich bringen kann.

Bei Berücksichtigung aller hier aufgeführten Kriterien kommt bei der Notwendigkeit des Abschlusses einer Vereinbarung zur Auftragsverarbeitung in einer Bildungseinrichtung entweder die Auswahl eines organisationsinternen Messengers in Frage oder das Auftragshosting oder gar Eigenhosting eines anbieterunabhängigen Systems.

Der Fokus der vorliegenden Studie, besonders Messenger im Sample zu untersuchen, die für Privatpersonen frei erhältlich sind, erwies sich also unter dem Aspekt der möglichen Notwendigkeit des Abschlusses einer solchen Vereinbarung möglicherweise als problematisch. Im Verlauf der Recherche zeigte sich unter der unter Anforderungen genannten Anforderung an Geheimhaltungen, dass die Anforderungen an den Einsatz einer Messenger-App im Bildungskontext hoch sind. Will man alle Schweige- und Geheimhaltungspflichten berücksichtigen, so kommen nur solche Apps in Frage, mit denen die Bildungseinrichtung eine Vereinbarung zur Auftragsverarbeitung abgeschlossen hat. Hält man sich jedoch vor Augen, dass und wie leichtfertig in vielen Schulen und Bildungseinrichtungen – insbesondere vermehrt während der COVID-19-Präventionsmaßnahmen – zwischen Lehrenden und Lernenden per unverschlüsselter kommerzieller E-Mailanbieter kommuniziert wurde, revidiert sich der Anspruch auf die tatsächliche Vereinbarung einer Auftragsverarbeitung: Es scheint vielfach in Schulen und Bildungseinrichtungen über die privaten E-Mail-Adressen der Lernenden kommuniziert zu werden, und zwar ohne Verschlüsselung. Von den Lernenden scheint auch oft verlangt zu werden, zur Anmeldung in einem schulischen System einer Lernplattform (z.B. moodle) eine E-Mail-Adresse anzugeben (beispielhaft: Integrierte Gesamtschule Zell 2020), auch Hausaufgaben wurden per E-Mail versendet. Wenn hier keine Verschlüsselung erfolgt, dann liegen alle Inhalte und Namen in Klarversion bei den jeweiligen E-Mail-Anbietern vor, das sind oft datenauswertende Anbieter, meist auch auf ausländischen, oft US-amerikanischen Servern, z.B. Gmail (ZEIT ONLINE 2019), YahooMail, Hotmail, aber auch GMX-Mail analysiert gegebenenfalls die Inhalte von

Emails im „intelligenten Postfach“ (<https://www.gmx.net/mail/intelligentes-postfach/>). Es steht also hier in Frage, ob demgegenüber nicht die Verwendung eines DSGVO-konformen frei verfügbaren Messengers, der Ende-zu-Ende-Verschlüsselung aller Inhalte anbietet, nicht sinnvoller ist – auch ohne Vereinbarung zur Auftragsdatenverarbeitung. Hier kämen beispielsweise Threema, Wire, Chiffry, Ginlo (die letzteren drei leider mit der Notwendigkeit der Angabe eines personenbezogenen Datums wie E-Mail-Adresse oder Telefonnummer) und jene anbieterunabhängige Chat-Programme/-Apps, die einen sicheren Server nutzen.

5.2 Barrierefreiheit/-armut

5.2.1 Grundlagen

Grundlage für die hohe Relevanz der Berücksichtigung von Barrierearmut und somit der Entwicklung von Prüfkriterien sind:

1. UN-Behindertenrechtskonvention (UN-BRK), Art. 9, 21, 22, 24, verbunden mit Vorgaben aus Sozialgesetzbüchern zu Jugendhilfe (SGB 8) und Inklusion (SGB 9)
2. Barrierefreie-Informationstechnik-Verordnung (BITV) 2.0
3. Intuitive Bedienung
4. Zielgruppenspezifische Bedarfe (z.B. Lese-/Schreib-/Sprachschwierigkeiten)

Zu 1 und 2: Nach der ratifizierten UN-BRK müssen digitale Informationen und Informationstechnologien für alle Menschen zugänglich sein: Art. 9 (1): „Um Menschen mit Behinderungen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen, treffen die Vertragsstaaten geeignete Maßnahmen mit dem Ziel, für Menschen mit Behinderungen den gleichberechtigten Zugang zur physischen Umwelt, zu Transportmitteln, Information und Kommunikation, einschließlich Informations- und Kommunikationstechnologien und -systemen ... zu gewährleisten“. Hieraus kann abgeleitet werden, dass auch in der Schule und in anderen Bildungseinrichtungen die Zugänglichkeit zu allen Informationen und allen Informations- und Kommunikationstechnologien

gewährleistet sein muss. Zudem müssen Bildungsangebote sowie die dort genutzten Kommunikationsformen und Kommunikationsmittel für alle Menschen nutzbar sein (vgl: Art. 24 (3, c): Die Vertragsstaaten stellen sicher, „dass blinden, gehörlosen oder taubblinden Menschen, insbesondere Kindern, Bildung in den Sprachen und Kommunikationsformen und mit den Kommunikationsmitteln, die für den Einzelnen am besten geeignet sind“ vermittelt wird). Der schulische Einsatz einer Messenger-App, die beispielsweise nicht von blinden SchülerInnen zur gemeinsamen Kommunikation genutzt werden kann, könnte demnach als unzulässig interpretiert werden, wenn das die SchülerInnen bei den bildungsbezogenen Kommunikationsprozessen benachteiligt. Weitere und konkrete Vorgaben dazu macht die Barrierefreie-Informationstechnik-Verordnung (BITV) 2.0, die aber bislang wenig spezifisch für Apps ist und eher für Webseiten Vorgaben macht. BITV 2.0 soll eine umfassend und grundsätzlich uneingeschränkt barrierefreie Gestaltung moderner Informations- und Kommunikationstechnik gewährleisten (§ 1). Sie gilt insbesondere für Websites, mobile Anwendungen, elektronisch unterstützte Verwaltungsabläufe und grafische Programmoberflächen (§ 2). Für Angebote der Länder gelten eigene Bestimmungen. Durch die Verordnung wird die Richtlinie (EU) 2016/2102 umgesetzt.

Für die Entwicklung von Kriterien für Apps ist die Nutzung einer an der TU Dortmund entwickelten Leitlinie zur Bewertung von Apps hilfreich: Beispiele für Kriterien zur Barrierearmut sind Bedienbarkeit, Erlernbarkeit, Oberflächenästhetik, Inhalt, Zweckmäßigkeit (Reh@pp-Quality 2016). Kriterien für die Bedienbarkeit sind beispielsweise die Varianz von Einstellungsmöglichkeiten: Können Einstellungen zu Barrierearmut individuell getätigt oder assistive Technologien mit der Software kombiniert werden (entsprechend SGBIX §84 haben behinderte Menschen Anspruch auf barrierefreie Computer als Hilfsmittel)? Ist eine Nutzung ausschließlich auf Smartphones oder auch anderen Endgeräten möglich? Reagiert die jeweilige App auf die in den meisten Smartphones mittlerweile integrierten Bedienungshilfen? Lässt sich z.B. die Ansicht der Texte in der App mithilfe der Bedienungshilfen größer machen? Interaction Designer müssten hier mitgestalten und mit User-Testern, die

auf jeweilige Barrierefreiheit angewiesen sind, diverse Nutzungskontexte durchspielen.

Zu erwägen ist, ob aufgrund der sehr diversen Anforderungen durch diverse Sinneseinschränkungen (Hören, Sehen), Mobilitätseinschränkungen, verwendeter Assistenztechnologien etc. eine personenunabhängige Vorauswahl getroffen werden sollte, oder ob je nach Nutzenden eine App ausgewählt werden kann. Letzteres kann wiederum zu Problemen in der alltäglichen Anwendung führen, wenn Lehrende dieselben Inhalte auf verschiedenen Kanälen/Apps bereitstellen müssen.

Zu 3: Eine intuitive Bedienung ist notwendig dafür, dass nicht benachteiligte SchülerInnen zusätzlich benachteiligt werden, wenn die Kommunikationsmittel schwer zu erlernen und zu bedienen sind. Dies ist beispielsweise denkbar, wenn es bei Installationen bereits zu Schwierigkeiten kommen kann, wenn viele Bedienungsfehler auftreten, wenn Bedienungsweisen umständlich oder nicht intuitiv gestaltet sind. Dabei kann auch ein gegebenenfalls notwendiger Bezahlvorgang eine Rolle spielen.

Zu 4: Bei der Nutzung in Bildungseinrichtungen muss mit einem weiten Inklusionsbegriff (nicht nur auf Behinderungen bezogen!) bei der Prüfung der Barrierearmut gearbeitet werden wegen der zunehmend heterogenen Voraussetzungen und Bedarfe bei Kindern und Jugendlichen auch in Bezug auf ihre Hintergründe wie finanzielle Ausstattung, Bildungsstand, familiäre Erlaubnisse und Verbote, Sprachkenntnisse, Medienkompetenzen.

Die Berücksichtigung von Barrierearmut gestaltet sich in der Praxis als anspruchsvoll, insbesondere da die Nutzenden sehr unterschiedlich sind und ihre Bedarfe sich teilweise auch widersprechen können: Während es für seh-, lese- und lernbehinderte SchülerInnen notwendig ist, dass gesprochene Sprachnachrichten gesendet werden können, ist es für gehörlose SchülerInnen und LehrerInnen essentiell, dass solche nicht genutzt werden, sondern schriftlich oder durch videobasierte Gebärdensprache kommuniziert wird. Ideal ist aber, wenn der Messenger die Option für beides zur Verfügung stellt. Teilweise gibt es auch spezielle Versionen mit ausschließlich textbasierter Anzeige von Nachrichten.

Da die LehrerInnen und SchülerInnen unterschiedliche Betriebssysteme und -versionen verwenden, müssten die Verfügbarkeiten und Einstellungsmöglichkeiten und Reaktionen der Messenger-Programme für alle Varianten getestet werden.

5.2.2 Kriterien der Prüfung auf Barrierefreiheit

Aus den oben genannten Grundlagen entwickelten wir konkrete Kriterien, nach denen Messenger-Apps/-Programme einer Prüfung unterzogen werden können. Die jeweiligen Kriterien dazu sind in der Ergebnistabelle der publizierten Studie aufgelistet.

Die Auswahl der Kriterien erfolgte anhand grundlegender und wesentlicher Kriterien für barrierearme IT-Systeme/Apps (vgl. Oliveira 2016; Reh@pp-Quality 2016; Bundesministerium der Justiz und für Verbraucherschutz 2011; Aktion Mensch und Stiftung Digitale Chancen 2010). Zusätzlich führten wir mit Domingos de Oliveira, einem Experten für digitale Barrierefreiheit ein informelles Experteninterview. Aus diesen Informationen und den weiteren Quellen entwickelten wir teilweise spezifische Prüfkriterien für Messenger-Apps:

1. Bedienbarkeit und Steuerbarkeit (hier: Grundfunktion des Schreibens und Lesens sollen gegeben sein)
2. Verständlichkeit und Erlernbarkeit
3. Wahrnehmbarkeit (ausreichender Kontrast für Sehbehinderte bei den Bedienelementen) und Oberflächenästhetik (klares und einfaches Design zur Orientierung über die Bedienoberfläche)
4. Zugänglichkeit
5. Multimedia
6. Nachhaltige Nutzbarkeit bzw. Kompatibilität mit den in Smartphones integrierten Bedienhilfen

5.2.3 Zusammenfassung der Prüfung auf Barrierefreiheit

Die Barrierefreiheit der Messenger-Apps wurde nicht umfassend geprüft. Obwohl zu Beginn der Studie eine Prüfung unser Wunsch war, stellte sich bei der Erarbeitung der Kriterien sowie der ersten Prüfungsversuche heraus, dass dies im Rahmen der zeitlichen und finanziellen Beschränkungen des Projekts nicht leistbar war. Für sinnvolle Ergebnisse müsste jede App auf allen Betriebssystemen (iOS, Android und jeweils in verschiedenen älteren und neueren Versionen davon), mit Einschalten diverser Assistenz-Modi (z.B. für sehbehinderte, mobilitätseingeschränkte Nutzende etc.) geprüft werden. Hier bietet sich die Rückfrage z.B. bei Selbsthilfeverbänden – also bei direkt Betroffenen – an. Für den Bereich Sehbehinderung empfehlen betroffene IT-Experten WhatsApp und Threema (Zehe 2018), vom Bayerischen Blinden- und Sehbehindertenbund e. V. liegt uns eine Stellungnahme vor, dass die Barrierefreiheit für Sehbehinderung bei Threema „definitiv gegeben ist“ (A. Pavkovic, pers. Komm. 2021). Die Messenger-Apps sollten von ExpertInnen der Barrierefreiheit geprüft werden. Da wir uns dazu nicht in der Lage sahen, prüften wir eher die Praktikabilität der Apps und stellten uns dabei spätere NutzerInnen vor, die wenig technikversiert sind. Daher übernahmen wir für die Testung der Praktikabilität teilweise Kriterien der Barrierefreiheit wie Bedienbarkeit und Steuerbarkeit sowie Oberflächenästhetik mit dem Ziel zu prüfen, ob ein Umstieg auf eine neue App für wenig technikversierte Menschen mit wenig Lernaufwand aussichtsreich erscheint.

Ein Fazit können wir aber bereits ziehen: Es gibt nicht DIE eine barrierefreie Messenger-App – ein für hörbehinderte Menschen gut geeigneter Chat-Client muss nicht zwangsläufig auch für lernbehinderte Menschen gleichermaßen geeignet sein.

Empfehlung:

Für kleinere Bildungseinrichtungen kann daher empfehlenswert sein, je nach Zusammensetzung und Bedarfen (an Sehen, an Sprache und Lesefähigkeiten etc.) der Lernenden und Lehrenden eine Messenger-App auszuwählen. Insgesamt könnte es lohnenswert sein, wenn die großen Träger von Bildungseinrichtungen gemeinsam eine quelloffene App auswählen, die sich dann je nach Bedarf an Barrierefreiheit weiterentwickeln und anpassen ließe, ohne dass man sich von den Entwicklungen der Herstellerfirmen abhängig macht. Gleichzeitig kann dies dann wieder der Allgemeinheit zugute kommen.

5.3 Praktikabilität

Eine datensichere, barrierearme App muss nicht automatisch auch zum beabsichtigten Nutzungserfolg in einer Organisation führen. Unter anderem ist auch relevant, ob Menschen diese App als praktisch erleben, ob sie die App mögen, ob sie gewohnte oder zusätzliche nützliche Features bereitstellt, ob sie sich gut in weitere Organisationsabläufe der Einrichtung einfügt und vieles mehr. Daher wurden weitere Kriterien für ihre Praktikabilität entwickelt. Eine App, die unpraktisch im Handling ist oder die aufgrund von Einschränkungen nicht den gewünschten Nutzungserfolg erzielen kann, wird sich in der Praxis bei den Nutzenden nicht durchsetzen können – es besteht dann ein hohes Risiko, dass die Lernenden eben doch selbständig eine informelle WhatsApp-Gruppe einrichten und darüber kommunizieren. Insbesondere diese dritte Kategorie der Praktikabilität enthält somit Aspekte, die sich auf die spezifische Arbeit in Bildungseinrichtungen beziehen und den inklusiven Auftrag der Bildungseinrichtungen zum Umgang mit diversen Menschen unter den Lernenden und Lehrenden berücksichtigt. Auch mit diesem Fokus fanden wir relevante Kriterien, die bislang in herkömmlichen Prüftabellen kaum entwickelt und abgebildet sind.

5.3.1 Grundlagen

Während die vorherigen zwei Prüfkriterien eher auf rechtlicher Basis fundierten, ist dies bei Praktikabilität nicht so; hier geht es um den Funktionsumfang und um notwendige Konzepte der Einbindung in die Bildungseinrichtung, die u.a. abhängig vom Verwendungskontext sind.

Darüber hinaus sind auch konzeptuelle Möglichkeiten der Einführung und Integration der App in der Institution bzw. Organisation zu klären. Diese sind teilweise von Merkmalen der App abhängig (z.B. Mindestsystemanforderungen, Altersfreigabe). Teilweise sind sie aber auch unabhängig von den Merkmalen einer spezifischen App zu klären, beispielsweise bei der Frage ob und wie es sich lohnt, durch die Einführung einer Alternative zum WhatsApp-Messenger überhaupt Mehrwerte zu generieren, wenn der Mehrwert der bereits erfolgten Verbreitung der App nicht gegeben ist. Dafür sollten Konzepte zur Einführung, Nutzung und gegebenenfalls Weiterbildung sowie didaktische Konzepte zur Nutzung in Kommunikations- und Lehrkontexten geplant werden. Insbesondere kann hier auch auf technische und organisatorische Vorteile (aber auch Kostenvorteile) hingewiesen werden, die dann einen tatsächlichen Mehrwert darstellen.

5.3.2 Kriterien der Prüfung

Funktionsumfang und Merkmale mit Ausprägungen einzelner Messenger:

1. NutzerInneneigenschaften/Alter:

Wie lässt sich das erlaubte Nutzungsalter einer App herausfinden? In den App-Stores wird beispielsweise für WhatsApp die Altersfreigabe „USK 0 Jahre“ angegeben. Die Unabhängige Selbstkontrolle (USK) der Medienwirtschaft ist hier aber nicht rechtlich bindend, sondern die Allgemeinen Geschäftsbedingungen (AGB). Diese orientieren sich an der DSGVO. Die Altersfreigabe für WhatsApp und alle andere Messenger, die personenbezogene Daten erheben, ist in Deutschland 16 Jahre. Personenbezogene Daten sind beispielsweise eine anzugebende

Telefonnummer oder E-Mail-Adresse für die Anmeldung. Von jenen Messengern, die oben als DSGVO-konform angegeben wurden, erfordern SID und Wire die Angabe der E-Mail-Adresse. Somit ist von proprietären Systemen nur Threema für Kinder jünger als 16 Jahre ohne Einverständniserklärung der Erziehungsberechtigten nutzbar.

2. Finanzierung:

Ist ein Messenger kostenfrei oder kostenpflichtig nutzbar? Eine als sicher einzustufende und viele Merkmale erfüllende App wie Threema ist kostenpflichtig. Sie kostet einmalig 3,99 Euro. Dies ist zwar nur etwa so viel wie ein Cappuccino, jedoch stellt der Bezahlvorgang an sich für viele AdressatInnen eine große Hürde dar, wenn sie keine Kreditkarte besitzen, keine Daten von sich preisgeben möchten oder nur geringe Nutzungsfertigkeiten besitzen. Es lassen sich aber von der Organisation Lizenzen kaufen und an spätere Nutzende verschenken. Bei anbieterunabhängigen Messengern sind die meisten Apps/Programme kostenlos – es gibt jedoch auch die Möglichkeit individuellem „Branding“ und des eigenen Serverbetriebs, was natürlich nicht kostenfrei möglich ist.

3. Interne und externe Nutzung:

Ermöglicht der Messenger die Kommunikation nur innerhalb des Einrichtungskontexts oder kann er von den Nutzenden auch für private Kontakte genutzt werden?

4. Features:

Werden beliebte Features wie Anrufe, Videochat, Gruppenchat (alles verschlüsselt) angeboten? Gibt es Einschränkungen beim Versand von Videos, Bildern, Sprachnachrichten? Dies kann die Akzeptanz und Alltagsintegration mit beeinflussen.

5. Technischer Aufwand der Betreuung und Nutzung:

Hier ist zu prüfen, ob die Nutzung für die späteren Nutzenden technisch unaufwändig erscheint (Finanzierung; Auftragshosting) und ob der Betrieb technische Wartung und somit Personal erfordert, wie es beispielsweise

bei einem organisationseigenen Serverbetrieb (z.B. bei Mattermost oder XMPP-Server) der Fall wäre und ob dies kostengünstiger als Lizenzlösungen wäre.

6. Server: Eigener Serverbetrieb möglich?
7. Betriebssysteme:
Kompatibilität mit allen gängigen Betriebssystemen, auch älteren Versionen ist notwendig, wenn die Nutzenden ihre eigenen Geräte nutzen sollen, die nicht reguliert werden können.
8. Desktopversion:
Ist für die Nutzung ein Smartphone notwendig oder lässt sich mit der Software auch über Computer und ohne SIM-Karte kommunizieren? Dies hat den Vorteil, dass AdressatInnen Computer nutzen können, die in der Einrichtung zur Verfügung gestellt werden können und ein Handy-Kauf nicht notwendig ist, um an der Kommunikation teilhaben zu können, wenn beispielsweise Eltern/Erziehungsberechtigte kein Handy erlauben. Auch kann für Fachkräfte die Dokumentation durch die Desktopnutzung samt Drucker erleichtert werden.
9. Integration in bestehende Softwarenutzungen:
Ist die Messenger-App kompatibel mit anderen softwaregestützten Kommunikations- und Organisationsabläufen und ohne dauerhaften Mehraufwand integrierbar?

Die folgenden Aspekte und Kriterien erlauben keine Angabe von Merkmalsausprägungen für einzelne Apps. Sie sind eher Kriterien, die es zu bedenken gilt bei der Entscheidung, ob und wie und unter welchen Bedingungen ein Messenger-Einsatz in der Bildungseinrichtung erfolgversprechend geplant werden kann. Hier müssen Vorgehensweisen und Relevanzen priorisiert werden und Konzepte für die potenzielle Einbindung des Messengers in die Organisationsstruktur der Bildungseinrichtung entsprechend der Schulgesetze geplant werden:

10. Wie können Nutzende motiviert werden, die Software in ihre Alltagspraxis zu integrieren, insbesondere, wenn sie möglicherweise bereits eine Alltagspraxis für die Kommunikation mit einem anderen Messenger (häufig WhatsApp) entwickelt haben und es explizite oder gewohnheitsbedingte Widerstände bei der Akzeptanz gibt?
11. Einverständniserklärungen:
Müssen die Nutzenden bei den Herstellern oder bei der Organisation ihr Einverständnis erklären? Was passiert, wenn sie dies nicht tun möchten?
12. Gerätebesitz, Dienstgeräte:
Welche Geräte können verwendet werden? Können/müssen private Geräte verwendet werden oder können/sollten Geräte durch die Einrichtung bereitgestellt werden?
13. Weiterbildungsbedarfe, Abläufe:
Ergeben sich Weiterbildungsbedarfe für Fachkräfte oder AdressatInnen? Ist die Software selbsterklärend? Verändert die Nutzung Arbeitsabläufe oder Kommunikations-, Dokumentations- oder Organisationsstrategien, die es zu klären gilt? Sind Chatadressen organisationsbezogen (funktions-, aufgaben- und personenbezogen) möglich?

5.3.3 Ergebnisse der Prüfung auf Praktikabilität

Die Merkmalsausprägungen der DSGVO-konformen Messenger wurden recherchiert und in der Ergebnistabelle festgehalten und notiert. Ob und wie diese Merkmalsausprägungen bedeutsam sind, kann nicht positiv oder negativ bewertet werden, es ist vielmehr vom Einsatzkontext und vom Konzept in der Bildungseinrichtung abhängig. Die Entwicklung der Kriterien diene somit weniger der Prüfung, sondern mehr als Informationsquelle der Sichtbarmachung der Unterschiede der Messenger, sodass konzeptionelle Entscheidungen aufgrund der Merkmale überhaupt erst möglich werden. Die Prüfkriterien erfüllen ihren Zweck somit besonders in der eigenen Anwendung. Dies gilt insbesondere für die Testung der Praktikabilität – diese zeigte auf, worauf bei der Einführung eines Messengers in

Bildungseinrichtungen Wert gelegt werden kann. Meist ist nämlich nicht vorab auf den Herstellerseiten erkennbar, ob und wann beispielsweise Daten bei der Installation angegeben werden müssen oder was das Mindestalter ist. Im Kontext der beruflichen Bildung für Erwachsene ist ein Mindestalter von 16 Jahren weniger relevant als in einem Bildungskontext, bei dem Kinder und Jugendliche unter 16 Jahren erwartet werden.

Bei diesem Vorgehen des Ausprobierens der diversen Messenger im Studententeam wurde ersichtlich, wie bedeutsam einzelne Eigenschaften und Vorgehensweisen einer App sein können, die auf Herstellerseite oder konventionellen Vergleichstabellen nicht immer transparent angegeben werden. Die Erkenntnisse des Ausprobierens mündeten teilweise iterativ in der Entwicklung eines weiteren zusätzlichen Prüfkriteriums Praktikabilität, welches dann für die bereits geprüften Apps erneut recherchiert wurde.

6 Ergebnisse III: Potential von freien anbieterunabhängigen Messengern mit auftrags- oder eigengehosteten Chatservern

Neben den anbieterabhängigen (firmeneigenen) Messenger-Apps der Gruppen A und C von einzelnen Herstellern gibt es auch freie Messenger-Systeme, die auf dem internationalen Standard „XMPP“ oder auf dem Matrix-Protokoll basieren (Gruppe B). Im Zuge der Entwicklung von Kriterien für Datenschutz, Barrierefreiheit und Praktikabilitätsanforderungen von Messengern in Bildungseinrichtungen wurden die potenziellen praxisbezogenen Vorteile freier Messenger-Systeme deutlich. Diese können im Rahmen der Studie nur in wenigen Aspekten geprüft werden, da insbesondere der Datenschutz vom Serveranbieter abhängt. Darin liegt aber ihr Potenzial, das hier kurz mit dem Ziel einer Einordnung beschrieben werden soll (für einen guten Überblick und Einführung sowie Hinweise auf weitere Quellen vgl. Initiative Freie Messenger o.J.a; Werz 2019):

Hierzu gehören u.a.:

- mehrere voneinander getrennte Chatkonten (Beruf, Privat, Verein, Sonstiges, ...) sind möglich;
- sie sind sowohl mit als auch ohne SIM-Karte nutzbar;
- mehrere Endgeräte können synchron genutzt werden;
- je nach Server ist die Errichtung eines Chat-Kontos ohne personenbezogene Daten und somit auch für Kinder möglich;
- wie bei E-Mail gibt es textbasierte Chat-Apps, die für Barrierefreiheit bei Sehbehinderung sorgen, da sie für Screenreader optimal sind.

Worin liegt der wesentliche Unterschied zwischen anbieterunabhängigen, freien Messengern und den bekannten anbieterabhängigen?

WhatsApp-Nutzende können nur mit WhatsApp-Nutzenden und Threema-Nutzende nur mit Threema-Nutzenden kommunizieren. Anbieterunabhängige Messenger sind offen und NutzerInnen können von allen entsprechend miteinander föderierten Servern unabhängig von ihrer präferierten Messenger-App kommunizieren.

Während die Entscheidung für eine anbieterabhängige Messenger-App allen Beteiligten der Bildungseinrichtung vorgibt, welche App sie nutzen müssen, lässt die Entscheidung für ein freies Messenger-System, das entweder auf dem XMPP-Protokoll oder auf dem Matrix-Protokoll basiert, den Nutzenden

Auswahlmöglichkeiten in vielerlei Hinsicht. Es ermöglicht sogar, dass ein Kommunikationsserver nicht nur auftragsbezogen, sondern auch selbst gehostet werden kann (beispielsweise über einen Landesserver für Schulen oder einen Server eines Bundesverbands der Wohlfahrtsverbände) und somit die Daten nicht zu einem anbietenden Dritten gelangen. Auch Datensicherungen lassen sich bei Auftrags-/Eigenhosting (ähnlich wie bei E-Mail) leicht machen. Es lässt sich mit der Kommunikation via E-Mail vergleichen:

Alle E-Mail-NutzerInnen können bekanntlich mit allen anderen E-Mail-NutzerInnen E-Mails austauschen, obwohl alle NutzerInnen unterschiedliche Anbieter und unterschiedliche Software benutzen. Unabhängig davon, welche E-Mail-Adresse genutzt wird (ob eine E-Mail-Adresse vom Arbeitgeber, von der Schule, von GMX, von Goglemail oder von einem datenschutzwerbenden Anbieter wie Posteo

stammt) und unabhängig davon, welche Software jemand zum Schreiben und Speichern verwendet (z.B. die GMX-Software oder den freien Thunderbird-Client oder den proprietären Outlook-Client auf dem Desktop oder das sichere kostenlose K9-Mailprogramm für das Android-Handy): Alle können einander Nachrichten schreiben. Wer auf Sicherheit und Verschlüsselung Wert legt, installiert zusätzlich noch eine Verschlüsselungssoftware wie PGP-Open für sein E-Mail-Programm. Nach diesem Muster funktioniert anbieterunabhängiges Chatten: Alle wählen ihren präferierten Server, von dem sie eine Chatadresse erhalten und wählen ihre präferierte Messenger-App (die vom Server unabhängig ist). Wer auf eine bestimmte Funktion Wert legt, wählt beispielsweise eine andere Messenger-Klienten (App/Programm) als jemand, der eine bessere Barrierefreiheit für die eigenen Bedarfe benötigt oder jemand, der seine Telefonnummer (als Teil der Chatadresse) preisgeben möchte.³

Eine Bildungseinrichtung, ein Schulverbund oder sogar ein übergreifender Landesserver stellen die Serverinfrastruktur dafür bereit, auf der alle ohne Zugriff von Dritten kommunizieren. Dennoch ist Kommunikation auch mit externen Kontakten möglich, die andere Server nutzen: Anders als bei den proprietären, von einer Institution zu erwerbenden Pro-Versionen wie school.cloud etc., können diese Messenger dann auch zusätzlich für die private Kommunikation mit Familie und Bekannten genutzt werden. In der Regel erlauben diese Messenger-Apps auch das Anlegen mehrerer Chatkonten in einer App um z.B. Schulisches von Privatem zu trennen.

Sowohl die Serversoftware (Initiative Freie Messenger 2020a) als auch die Messenger-Apps (z.B. Monal für iOS, Conversations für Android, Gajim für Windows, für einen umfassenden Überblick der Softwares siehe Initiative Freie Messenger

³ Aus Gründen der Praktikabilität wäre möglicherweise für eine supportpflichtige Bildungseinrichtung empfehlenswert, für die großen Betriebssysteme je eine Messenger-App zu empfehlen, sodass professioneller und kollegialer Support bewältigbar bleiben

o.J.b) sind kostenlos und meist quelloffen, so dass Anpassungen beispielsweise für noch mehr Barrierefreiheit oder Individualisierungen möglich sind.⁴ Diese können als Entwicklungsauftrag oder evtl. auch mit eigenen Ressourcen umgesetzt werden. Öffentliche Gelder (von Schulen) fließen so in die Erstellung von öffentlichem Code. Die Ergebnisse eigener Tests finden sich in der publizierten Ergebnistabelle im Reiter Praktikabilität. Mit neuesten Erkenntnissen würden wir inzwischen zusätzlich auch die Prüfung von „Siskin IM“ und „Monal“ für iOS Geräte empfehlen.

Zusammengefasst lassen sich folgende potenzielle Vorteile markieren:

Technisch:

- Es sind getrennte (und mehrere) Chatkonten möglich;
- gleichzeitige Nutzung von Mobilgeräten und Desktop/Laptops mit Nachrichtensynchronisation über mehrere Endgeräte;
- Chatten mit oder gänzlich ohne Smartphone;
- Chat-Clients für Windows/Linux/Mac sowie Android/iOS;
- keine personenbezogene System-Identifikations-Nummer;
- nicht nur geschlossene Chatgruppen, sondern auch öffentliche Chaträume sind möglich;
- vollständig quelloffener Programmcode von Clients und Serversoftware, der geprüft, individuell angepasst und frei weiterentwickelt werden kann.

Organisatorisch:

- „IT folgt Organisation“; individuelle Bezeichnung der Chatkonten möglich;
- Individualisierung („Branding“) möglich;
- bei selbst betriebenen Chatservern können die Daten in einem Sicherungskonzept berücksichtigt werden;

⁴ Für eine Installationsanleitung siehe (Grupp 2018).

- Anbindung an Nutzerverwaltungssysteme (z.B. LDAP) ist möglich;
- bei anbieterunabhängigen Systemen müssen keine Lizenzen erworben, verteilt und verwaltet werden, weil es kostenlose Apps zum beliebigen Download gibt (aber Chat-Konten müssen vergeben werden);
- Auftragsdatenvereinbarungen können geschlossen werden.

Kosten:

- Lizenzkostenfreie Software ist sowohl für Nutzer als auch für die Serverseite als Open Source vorhanden.
- Gelder können individuell für Programmieraufträge zur Verbesserung des Codes vergeben werden.
- Serverbetriebskosten fallen an.

Aber auch freie Systeme haben Nachteile:

- Die verschiedenen Clients für unterschiedliche Betriebssysteme haben (wie unterschiedliche Textprogramme, Browser, E-Mail-Programme usw. auch) keine einheitliche Benutzerführung. Jeder Nutzer kann/muss sich seine App selbst wählen.
- Die Entwicklung wird von vielen unterschiedlichen Personen mit unterschiedlichen Interessen vorangetrieben.
- Es gibt keine zentrale, koordinierte Finanzverwaltung.
- Es werden bislang zu wenig Entwicklungsaufträge vergeben, sodass die Projekte weniger finanzstark sind.
- Die Funktionsvielfalt ist bei jedem Client anders.

Die Funktionsvielfalt sowie die Benutzerfreundlichkeit unter Android, Windows und Linux ist größer/besser als unter iOS.

7 Auswahlentscheidungen für die Messenger-Dienste “Wire” und “Threema Work” für berufliche Bildung im Projekt IDiT

Das Projekt IDiT durchlief zwei praktischen Phasen, in denen die entwickelten Konzepte zur Vermittlung von Medienkompetenz an RehabilitandInnen, zum Einsatz von Messengern in der beruflichen Bildung und zur Arbeit in inklusiven Tandems am BFW Köln erprobt wurden. In den beiden Phasen sollten zwei unterschiedliche Messenger-Dienste zum Einsatz kommen, um Erfahrungen und Erkenntnisse zu zwei verschiedenen Apps generieren zu können. Dieses Kapitel stellt dar, aufgrund welcher Entscheidungsgrundlagen und Auswahlprozesse in den beiden praktischen Erprobungsphasen des Projekts die Messenger-Dienste Wire beziehungsweise Threema Work verwendet wurden.

7.1 Einschlusskriterium: Individuelle Nutzbarkeit

Wie oben (3.3) dargestellt, lässt sich unterscheiden zwischen individuell nutzbaren Messenger-Diensten (Gruppe A und B) und solchen in Gruppe C, die in Form von Lizenzen von einer Einrichtung/Organisation zur Verfügung gestellt werden müssen (hier: „institutionsintern“).

Diese institutionsinternen Messengersysteme (Gruppe C) können Vorteile gegenüber den anbieterabhängigen individuellen Messengern (Gruppe A) bieten: etwa durch ihre schnelle und effiziente Verteilung von Lizenzen an die Lernenden, durch eine zentrale Verwaltung von Gruppen durch Lehrende/Administratoren, sowie durch die Möglichkeit des Abschlusses einer Auftragsverarbeitungsvereinbarung zwischen Bildungseinrichtung und Messenger-Dienst, die sicherstellt, dass die Pflicht zum Schutz personenbezogener Daten, die die Bildungseinrichtung gegenüber ihren Angestellten und Lernenden hat, auch durch Dritt-Verarbeitende, wie etwa einen Messengerdienst, gewahrt ist.

Institutionsinterne Messengerdienste wurden zunächst im Projekt IDiT nicht näher betrachtet oder in die engere Auswahl für den praktischen Einsatz genommen. Im Gegenteil: Das erste Einschluss-Kriterium war die individuelle (und eben nicht

organisationsabhängige) Nutzbarkeit der untersuchten Messenger-Dienste. Das zweite Einschlusskriterium war die Konformität zur DSGVO ohne erweiterte Einwilligungen. Daher wurden die anbieterunabhängigen Messenger (Gruppe B) nicht verfolgt, da kein eigenes Hosting möglich war.

Die Gründe hierfür liegen in der Grundkonzeption des Messenger-Einsatzes im Projekt: Das Forschungsinteresse lag primär auf der Frage, wie Messenger-Dienste als informelle Ergänzung und freiwilliges Zusatzangebot in der beruflichen Bildung eingesetzt werden können, nicht auf ihrem Einsatz als formal-verpflichtender Teil der Ausbildung. Es ging außerdem weniger darum, bestehende Angebote von Messenger-Diensten für Bildungskontexte auf Tauglichkeit zu prüfen, sondern mehr um die ganzheitliche Förderung der Medien- und Messengerkompetenz Lernender (Teilbereich: Kommunikation, Datenschutz). Genauer: Anspruch und Ziel war es, an der alltäglichen Nutzung von Messengern – meist überwiegend WhatsApp – anzusetzen, und alternative, datenschützende Messenger-Dienste zu identifizieren, die die Lernenden zur Vernetzung untereinander und mit ihren Ausbildenden, aber eben auch privat, und zwar auch mit Menschen außerhalb ihrer Bildungseinrichtung, nutzen können sollten.

Gleichzeitig sollten durch Aufklärung und Aufzeigen von Alternativen Denkprozesse bezüglich der eigenen Nutzung von Messenger-Apps angeregt sowie informierte Entscheidungen bezüglich der Auswahl von Apps auch für den privaten Bereich ermöglicht werden. Die Neu-Einführung eines Messengers geht dementsprechend im Konzept zu Messenger-Diensten als Kommunikations- und Vermittlungstool in der beruflichen Bildung (Murmans und Zorn 2021) und in dessen praktischer Erprobung am BFW Köln mit einer Aufklärung zu datenschutzrechtlichen Aspekten von Messenger-Diensten im Allgemeinen und den Risiken von WhatsApp im Besonderen einher.

7.2 Einschlusskriterium: Datenschutz

Unbedingte Voraussetzung für den Einsatz eines Messengers im Projekt IDiT war der Schutz personenbezogener Daten der Teilnehmenden (insbesondere, da diese

mit ihren privaten Smartphones teilnehmen). Da der Abschluss einer Auftragsverarbeitungsvereinbarung zwischen Bildungseinrichtung und Messengerdienst bei individuell nutzbaren Messengern nur teilweise möglich ist, war das zweite Kriterium für die Auswahl von Messengern für die praktische Erprobung die DSGVO-Konformität der Programme und Dienste. Damit einhergehendes Einschlusskriterium war die Verortung von Unternehmenssitz und Standort der Server in der EU, da dann die DSGVO unabhängig von zusätzlichen Vereinbarungen (wie etwa des im Sommer 2020 vom EuGH für ungültig erklärten Privacy Shields) greift.

Entsprechend war die engere Auswahl deckungsgleich mit jenen Messenger-Diensten, die anhand der in der Studie aufgestellten Kriterien als datenschutzgerecht identifiziert wurden (vgl. Kapitel 5.1.3):

- Threema
- Hoccer (inzwischen eingestellt)
- Wire
- SID (nur Betaversion verfügbar)
- Ginlo
- Chiffry

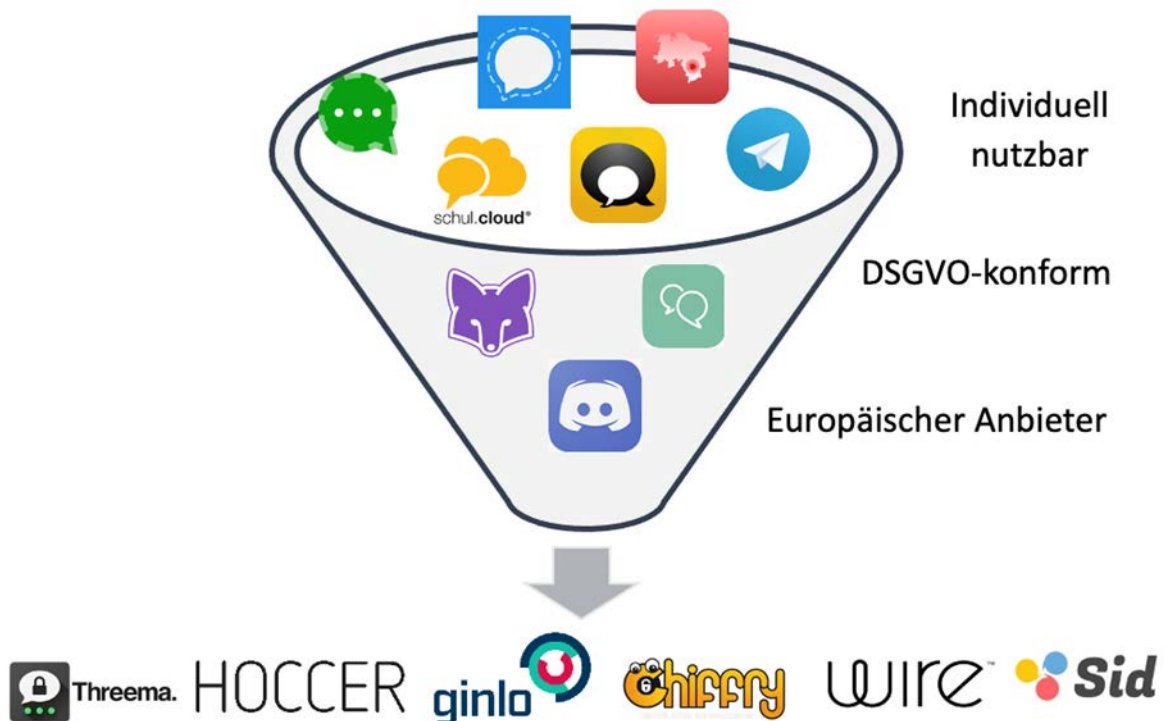


Abb. 2 Darstellung der Filterkriterien DSGVO-Konformität, Standort/Sitz in EU und individuelle Nutzbarkeit. Diesen Kriterien hielten Stand: Threema, Hoccer, Ginlo, Chiffry, Wire und SID, sowie anbieterunabhängige Messenger (aber nur in Verbindung mit einem gewerblichen Serveranbieter, der einen Vertrag zur Auftragsdatenverarbeitung ermöglicht, weshalb diese rein als App nicht näher betrachtet wurden).

7.3 Von der engeren Auswahl zu Wire und Threema (Praxistest)

Die sechs Messenger-Dienste, die aufgrund des in 7.1 und 7.2 dargestellten Auswahlprozesses die engere Auswahl bildeten, wurden von acht Projektmitarbeitenden über einen Zeitraum von zwei Monaten getestet.

Die Beobachtungen und Erkenntnisse aus der Testphase sind zusammengefasst im Reiter „5 Praxistest in IDiT“ der Ergebnistabelle (Zorn, Murmann, Harrach-Lasfaghi 2021b).

Folgende Beobachtungen und Erkenntnisse bezüglich der Apps der engeren Auswahl (Threema, Hoccer, Wire, SID, Ginlo und Chiffry) führten letztlich zur finalen Auswahl von Threema und Wire:

- SID entfiel, da sich die App zu diesem Zeitpunkt noch im Beta-Stadium befand, und sich dies durch gehäuft auftretende technische Mängel auch zeigte.
- Hoccer entfiel ebenfalls aufgrund mehrfach auftretender technischer Probleme (Nachrichten wurden nicht zugestellt/angezeigt; Absturz der App; keine Sprachnachrichten in bestimmten Smartphone-Versionen). Hoccer ist zudem seit April 2020 wegen Insolvenz nicht mehr existent.
- Ginlo: Lief nicht auf Android 4.5. Es wurde zudem während der Praxisphase des Projekts zwischenzeitlich eingestellt (Nov. 2019 bis Feb. 2020). Ist aktuell (Stand Februar 2021) überarbeitet und scheint vielversprechend – allerdings Desktopversion nur in der Business-Variante und keine App für Windows-Smartphones.
- Threema ist eine technisch ausgereifte App mit für Bildungskontexte hilfreichen Funktionen (z.B. Umfrage-Funktion, Desktop-Anwendung) und wurde für den Einsatz im Projekt ausgewählt.
- Chiffry: Verfügt nicht über die Funktion des Video-Anrufs. Verfügt nicht über eine Desktop-Version, war daher weniger gut geeignet für den pädagogischen Einsatz.
- Bei der Entscheidung für Wire spielte das ungewöhnliche Design/User-Interface eine Rolle. Die Abwägung zwischen dadurch potenziell erschwertem Zugang zur App einerseits und der Möglichkeit spielerischer und andersartiger Messenger-Kommunikation andererseits fiel zugunsten letzterer aus. Es schien reizvoll, den Teilnehmenden einer der beiden praktischen Durchgänge als Variante eine App anzubieten, die nicht dem gängigen Messenger-Design entspricht.

Damit wurde ein kostenloser Messenger-Dienst der Gruppe A (Wire, IDiT-Durchgang 1, Nov 2019 bis April 2020) und ein kostenpflichtiger, institutionell beschaffter Messenger-Dienst (Threema Work, IDiT-Durchgang 2, Nov. 2020 bis April 2021) (als Mischform der Gruppe A und C, weil er zwar institutionell beschafft ist, aber dennoch

individuelle Nutzung mit externen Threema-Nutzenden ermöglicht) ausgewählt. Wir verfügen über eine Altersbeschränkung und ist erst ab 16 Jahre zugelassen. Für den Projektkontext der beruflichen Rehabilitation spielte dies keine Rolle, es kann aber bei jüngeren Auszubildenden eine Rolle spielen, die unter 16 Jahre sind. Hier ist die Einverständniserklärung der Erziehungsberechtigten erforderlich. Die Altersbeschränkung resultiert aus der Erhebung der E-Mail-Adresse, hier ist auch bei über 16-Jährigen zu erwägen, eher auf die Pro-Version zurückzugreifen, um zum Schutz auch der Metadaten eine Vereinbarung zur Auftragsverarbeitung abschließen zu können.

7.4 Von Threema zu Threema Work

In IDiT-Durchgang 2 tatsächlich zum Einsatz kam statt Threema (individuell nutzbar) also letztlich Threema Work (organisationsabhängig). Ausschlaggebend für diese zunächst im Widerspruch zu den oben (7.1) dargelegten Überlegungen stehende Entscheidung war die Tatsache, dass Threema Work als App kompatibel ist mit der regulären Threema-App, die auch für Privatpersonen verfügbar ist. Dies bedeutet, dass Nutzende einer Threema-Work-Lizenz problemlos mit Nutzenden einer Threema-Lizenz kommunizieren können. Kontakte der regulären Threema-App werden in Threema Work als privat gekennzeichnet (Symbol: Haus); Kontakte aus Threema-Work werden in der regulären Version als beruflich gekennzeichnet (Symbol: Aktenkoffer).⁵

Damit greift der zentrale Grund, warum im Projekt nicht mit organisationsabhängigen Diensten gearbeitet werden sollte, für Threema Work nicht. Die Vorteile, die Threema Work gegenüber der regulären Threema-App besitzt, sind aber genau jene, die sonstige organisationsabhängige Messenger auch besitzen. Für IDiT spielte dabei insbesondere die schnelle und einfache Verteilung von Lizenzen an die

⁵ Ungeklärt blieb: Wie verhält sich das bei mehreren Arbeitgebern (was tatsächlich vorkommen kann)? Gibt es eine Trennung der jeweiligen Kontakte?

Teilnehmende eine wichtige Rolle. Die Kosten für die Lizenzen wurden vom Projekt getragen, und unter diesen Umständen war die Nutzung von Threema Work die für alle Beteiligten (Teilnehmende, Auszubildende, Projektmitarbeitende) effizienteste Lösung – bei gleichzeitigem Einlösen des Anspruchs, dass die App auch privat nutzbar sein sollte.

Übersicht: Vorteile von Threema Work gegenüber Threema

- Nutzerverwaltung via Manager-Cockpit: Das Management-Cockpit gibt eine Übersicht der aktiven Nutzer, deren IDs sowie der verwendeten Lizenzen.
 - Verwaltung der Zugangsdaten
 - Trennen von Threema-IDs
 - Löschen von Threema-IDs
- Individualisierung
 - In-App-Logo
 - interne Kontaktliste
 - Nutzer Support via In-App-Formular
- App-Konfiguration
 - Konfigurieren der App für Nutzer direkt im Management-Cockpit. Mit Threema-MDM können alle oder bestimmte Nutzer App-Einstellungen angepasst sowie gezielt Funktionen deaktivieren werden.
 - Statistiken: anonymisierte Datenauswertungen
 - Lizenzverwaltung
 - Verwalten von Zugriffsberechtigungen: Ernennen zusätzlicher Administratoren und Benutzer für das Management-Cockpit und Berechtigungen festlegen

7.5 Zusammenfassung: Auswahlentscheidungen eines Messengers für die berufliche Bildung im Projekt IDiT

Zusammenfassend ist festzuhalten: Für die Auswahl der Messenger, die in der Praxisphase des Projekts IDiT am Berufsförderungswerk Köln zum Einsatz kamen, waren ausschlaggebende Einschlusskriterien die DSGVO-Konformität der Programme sowie die Ansässigkeit der anbietenden Unternehmen und Standort der datenverarbeitenden Server in der EU. Aus konzeptionellen Gründen – der Leitgedanke war mehr die Förderung allgemeiner Medienkompetenz der Teilnehmenden, weniger das Prüfen bestehender Angebote von Messenger-Diensten für Bildungskontexte – wurde Wert gelegt darauf, dass ein Messenger auch privat und für die Kommunikation mit Menschen, die nicht zur eigenen Bildungseinrichtung gehören, nutzbar sein sollte. Daher wurden zunächst organisationsabhängige Messenger-Dienste ausgeschlossen.

Die finale Auswahl von Wire und Threema geschah auf Basis von Erkenntnissen eines projektinternen Praxistests, bei dem insbesondere Features, Praktikabilität und Design der Messenger fokussiert wurden. Zugunsten des Variantenreichtums im Rahmen des Forschungsprojekts wurde Wire trotz anfänglicher Bedenken zu möglichen Zugangsschwierigkeiten gerade wegen seiner eher untypischen Oberflächen-Ästhetik ausgewählt. Da Threema mit Threema-Work über ein Angebot verfügt, das einerseits die Vorteile organisationsabhängiger Messenger-Dienste bietet, andererseits aber mit der regulären Threema-App kompatibel und somit problemlos privat nutzbar bleibt, fiel hier die Entscheidung letztlich entgegen der ursprünglichen Annahme, organisationsabhängige Messenger auszuschließen, zugunsten von Threema Work aus.

Wie sich beide Messenger im praktischen Einsatz bewähren und wo offene Fragen entstehen sowie Herausforderungen und Chancen sichtbar werden, ist zu evaluieren.

8 Zusammenfassung

Der Beitrag schilderte die Bedarfe für Messenger-Kommunikation in Bildungseinrichtungen und ging der Frage nach, welche Kriterien bei Entscheidungen zur Messenger-Kommunikation im Berufsförderungswerk Diakonie Michaelshoven im Projekt IDiT zugrunde gelegt wurden. Dazu stellte der Beitrag systematisiert Anforderungen bei der Nutzung von Messengern in Bildungseinrichtungen dar, die sich von Anforderungen von Privatpersonen unterscheiden und entwickelte daraus drei Bereiche mit Kriterien, die es bei der Entscheidung für ein Messenger-Angebot zu prüfen gilt: Datenschutz, Barrierearmut, Praktikabilität für den Anwendungszweck. Mängel bei der Anwendbarkeit von DSGVO führen dazu, dass populäre Messenger nicht für den Einsatz in Schule oder Sozialer Arbeit geeignet sind⁶. Ein großes Problem beim Datenschutz ist der mangelnde Schutz der Adresseinträge auf einem Gerät sowie der Umgang mit Metadaten. Datenschutz alleine ist aber kein ausreichendes Kriterium. Bei den datensichereren Anbietern kann nach entwickelten Prüfkriterien Praktikabilität und Barrierearmut geprüft werden. Hier zeigen erste Recherchen und Prüfungen, dass mit DSGVO-Konformität (z.B. Threema, Wire, Hoccer, XMPP-basierte Apps) bereits Abstriche bei Praktikabilität und Barrierearmut einhergehen.

Interessante Alternativen existieren aber unter jenen Messengern, die mittels Verträge durch die Institution angeboten werden⁷ und bei denen im Vertrag Vereinbarungen zu Auftragsverarbeitung mit den Herstellern getroffen werden können. Ohne getroffene Vereinbarungen zur Datenauftragsverarbeitung mit den Herstellern/Serverbetreibern bewegt sich die Nutzung auch von freien Messengern

⁶ Z.B. WhatsApp, Telegram, Viber, Skype, Signal

⁷ Beispiele dafür sind Organisationslösungen wie Threema Work/Education, WeChat, Wire Pro/Enterprise, SchulCloud oder andere – aber auch anbieterunabhängige Messenger). Aus Gründen der Praktikabilität und der Akzeptanz könnte es sich lohnen darauf zu achten, dass damit nicht nur organisationsinterne Kommunikation möglich ist, sondern auch private Kommunikation – falls von Nutzenden gewünscht – damit getätigt werden kann.

durch Einrichtungen selbst bei DSGVO-Konformität (zumindest) in einer Grauzone, wenn es um Verschwiegenheitspflichten oder Sozialdatenaustausch geht. Es ist zu klären, wie dies bei Ende-zu-Ende-Verschlüsselung juristisch zu bewerten ist, wenn technisch bedingt nur die beiden Kommunikationspartner Zugriff auf die Kommunikation haben und vom Anbieter keine Metadaten gespeichert werden. Neben kostenpflichtigen Angeboten zum Auftrags-/Fremdhosting sowohl von Organisationslösungen als auch freien Messengersystemen besteht auch die Möglichkeiten des eigenen Serverbetriebs zur Verarbeitung der Daten mit z.B. Mattermost (quelloffene Teamlösung) oder normalen (ebenfalls quelloffenen) Chat-Servern auf XMPP-basis⁸.

Eine Excel-Übersicht über detaillierte Messenger-Recherchen entsprechend der aufgezeigten Anforderungen und Kriterien wurde im Rahmen des BMBF-geförderten Projekts IDiT erstellt (Zorn, Murmann und Harrach-Lasfaghi 2021b).

Die Weiterentwicklung von Kriterien für organisationale Umsetzbarkeit oder Praktikierbarkeit sollten daher in pädagogischen Kontexten nicht ausschließlich mit technischen, sondern auch mit pädagogischen Fachkräften erfolgen und geprüft werden, bevor organisationale Entscheidungen getroffen werden, weil Technikentscheidungen pädagogisches Handeln beeinflussen (Kutscher et al. 2020). Weil die zu treffenden Entscheidungen umfassend geprüft werden müssen und Auswirkungen auf Arbeitsabläufe haben, ist eine Entscheidung durch obere Hierarchieebenen anzuraten, da dies nicht einzelnen Fachkräften zugemutet werden kann.

Vermutlich ist eine technische Weiterentwicklung privatsphäreschützender Softwares für den in Frage stehenden Kontext notwendig, damit sie zunehmend auch die in den Punkten Barrierearmut und Praktikabilität beschriebenen Kriterien erfüllen können. Eine Zusammenarbeit auf Bundes-, Landes- oder Verbandebene und mit Stabstellen

⁸ https://www.freie-messenger.de/sys_xmpp/server/ ; Anleitung: https://www.freie-messenger.de/dateien/conversations/Anleitung_Conversations.PDF

der Landesdatenschutzbeauftragten sollte aufgrund der Komplexität erwogen werden. Zu überlegen ist zudem, ob nicht mit vielversprechenden und unkompliziert zu hostenden Open-Source-Produkten (evt. mit XMPP-Protokoll) verlässliche kostenlose Softwarealternativen durch die Länder oder durch Kooperationen der Wohlfahrtsverbände bereitgestellt werden könnten.

Fachkräfte und AdressatInnen würden so bei ihren Kommunikationsbedürfnissen unterstützt werden. Ein Nicht-Handeln der Einrichtungen verhindert zudem auch nicht grundsätzlich die Nutzung von Messengern. Vielmehr ist zu befürchten, dass dadurch die informelle Nutzung und Verbreitung jener Messenger zunimmt, die Daten nicht schützen, Privatsphäre nicht achten, Barrierefreiheit nicht respektieren und dass dies zunehmend zu Exklusionen führt, wenn beispielsweise Lernende untereinander trotz wachsenden Bewusstseins für Datenschutzfragen in Ermangelung von Alternativen resigniert dennoch per WhatsApp kommunizieren. Insofern sind die Bildungseinrichtungen hier auch entsprechend ihres Bildungsauftrags aufgefordert, Lösungen zu finden und anzubieten. Sie könnten durch das Aufzeigen der Machbarkeit datenschützender Messenger-Kommunikation die Medienkompetenz in den Dimensionen Medienkunde, Mediennutzung, Medienkritik und Mediengestaltung (Baacke 1996) eines breiten Bevölkerungsanteils fördern.

Ein Forschungsdesiderat für die Evaluierung von derartigen Feldforschungen wird deutlich. Weitere Forschung kann Erkenntnisse darüber liefern, wie Lernende mit WhatsApp-Alternativen kommunizieren und welche weiteren Aspekte und Kriterien somit Entscheidungen und Konzeptentwicklungen zur Messenger-Nutzung in Bildungseinrichtungen inspirieren sollten.

III Literaturverzeichnis

- Aktion Mensch und Stiftung Digitale Chancen. 2010. „Prüfschritte: Biene 2010 – Wettbewerb Barrierefreies Webdesign.“ Zugriff am 29. Januar 2021. <https://biene-award.de/pruefschritte/>.
- Baacke, Dieter. 1996. „Medienkompetenz - Begrifflichkeit und sozialer Wandel.“ In *Medienkompetenz als Schlüsselbegriff*, hg. v. Antje v. Rein, 111–23. Bad Heilbrunn. http://www.die-frankfurt.de/esprid/dokumente/doc-1996/rein96_01.pdf#page=111.
- Bos, Wilfried, Birgit Eickelmann, Julia Gerick, Frank Goldhammer, Heike Schaumburg, Knut Schippert, Martin Senkbeil, Renate Schulz-Zander und Heike Wendt, Hg. 2014. *ICILS 2013: Computer- und informationsbezogene Kompetenzen von Schülerinnen und Schülern in der 8. Jahrgangsstufe im internationalen Vergleich*. Münster: Waxmann. Zugriff am 8. Dezember 2016.
- Buchner, Benedikt. 2017. „DuD Recht AG Bad Hersfeld: Elterliche Pflichten bei WhatsApp-Nutzung der Kinder.“ *Datenschutz und Datensicherheit DuD* (9): 584-592.
- Cryptoparty. 2019. „cryptopartykbn:messenger.“ Zugriff am 13. Juni 2020. <https://www.cryptoparty.in/cryptopartykbn/messenger>.
- Datenschutzgrundverordnung. DSGVO. Europäisches Parlament. 27. April 2016. <https://dejure.org/gesetze/DSGVO>.
- Deutscher Berufsverband für Soziale Arbeit e.V. 2014. „Berufsethik DBSH.“ *Forum Sozial* (4): 3–43. <https://www.dbsh.de/media/dbsh-www/redaktionell/pdf/Sozialpolitik/DBSH-Berufsethik-2015-02-08.pdf>.
- Digitalcourage e.V. o.J. „Digitale Selbstverteidigung | Digitalcourage.“ Zugriff am 14. Juni 2019. <https://digitalcourage.de/digitale-selbstverteidigung>.
- Gebel, Christa, Gisela Schubert und Ulrike Wagner. 2015. „WhatsApp ist auf jeden Fall Pflicht“. Online-Angebote und Persönlichkeitsschutz aus Sicht Heranwachsender. Ausgewählte Ergebnisse der Monitoringstudie. München: JFF - Institut für Medienpädagogik in Forschung und Praxis. <https://www.pedocs.de/volltexte/2016/12614/>.
- Grupp, Andreas. 2018. „Conversations statt WhatsApp.“ Zugriff am 27. Juni 2020. <https://grupp-web.de/cms/2018/02/15/conversations-statt-whatsapp/>.
- Imort, Peter und Horst Niesyto, Hg. 2014. *Grundbildung Medien in pädagogischen Studiengängen*. München: kopaed.

- Incobs. 2015. „Barrierefreiheit von Messenger-Apps.“ Zugriff am 26. Juni 2020. <https://www.incobs.de/artikel/items/barrierefreiheit-von-messenger-apps.html>.
- Initiative D21 e.V. 2018. *D21-Digital-Index 2017/2018: Jährliches Lagebild zur Digitalen Gesellschaft*. 1. Auflage. D21-Digital-Index. Berlin: Initiative D21.
- Initiative Freie Messenger. o.J.a. „Freie Messenger.“ Zugriff am 1. Februar 2021. <https://www.freie-messenger.de/>.
- . o.J.b. „Jabber (XMPP).“ Zugriff am 1. Februar 2021. https://www.freie-messenger.de/sys_xmpp/.
- . o.J.c. „Matrix.“ Zugriff am 29. Januar 2021. https://www.freie-messenger.de/sys_matrix/.
- . 2020a. „Server.“ Zugriff am 1. Februar 2021. https://www.freie-messenger.de/sys_xmpp/server/#profitipp-eigener-server.
- . 2020b. „Warum nicht ... Übersicht über Messenger-Systeme.“ Zugriff am 15. Januar 2021. <https://www.freie-messenger.de/warumnicht/>.
- Integrierte Gesamtschule Zell. 2020. „Elternbrief - Digitale Lehr- und Lernsysteme im Schuljahr 20/21.“ Unveröffentlichtes Manuskript, zuletzt geprüft am 27. Januar 2021. https://www.igszell.de/wp-content/uploads/2020/08/digitale-lehr-und-lernsysteme-igs-zell-2020_21.pdf.
- Iske, Stefan und Nadia Kutscher. 2020. „Digitale Ungleichheiten im Kontext Sozialer Arbeit.“ In *Handbuch Soziale Arbeit und Digitalisierung*, hg. v. Nadia Kutscher, Thomas Ley, Udo Seelmeyer, Friederike Siller, Angela Tillmann und Isabel Zorn, 116–28. Weinheim [u.a.]: Beltz Juventa.
- Jin, Huafeng und Shuo Wang. 2017. Patent US00000010096319B1: Voice-based Determination of Physical and Emotional Characteristics of Users. US00000010096319B1. 15/457,846, eingereicht 13. März 2017, und veröffentlicht Oktober 9, 2018.
- Karaboga, Murat; Masur, Philipp; Matzner, Tobias; Mothes, Cornelia; Nebel, Maxi; Ochs, Carsten et al. (2014): White Paper Selbstdatenschutz. Hg. v. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt und Peter Zoche, Regina Ammicht-Quinn, Jörn Lamla, Alexander Roßnagel, Sabine Trepte, Michael Waidner. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Karlsruhe. Online verfügbar unter https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf, zuletzt geprüft am 03.10.2018.
- Klein, Alexandra und Caroline Pulver. 2019. „Professionalisierung in der Sozialen Arbeit.“ In *Handbuch Inklusion und Medienbildung*, hg. v. Ingo Bosse, Jan-René Schluchter und Isabel Zorn, 319–25. Weinheim [u.a.]: Beltz Juventa.

- Kuketz, Mike. 2020. „Conversations: Sicherer Android Messenger.“ Zugriff am 26. Juni 2020. <https://www.kuketz-blog.de/conversations-sicherer-android-messenger/>.
- Kutscher, Nadia, Thomas Ley, Udo Seelmeyer, Friederike Siller, Angela Tillmann und Isabel Zorn, Hg. 2020. *Handbuch Soziale Arbeit und Digitalisierung*. Weinheim [u.a.]: Beltz Juventa.
- Landesbeauftragte für den Datenschutz Niedersachsen. 2018. „Merkblatt für die Nutzung von "WhatsApp" in Schulen.“ <https://ipad-in-der.schule/wp-content/uploads/2018/12/Schreiben-Datenschutzbeauftragte.pdf>.
- Medienpädagogischer Forschungsverbund Südwest. 2017. „JIM-Studie 2017: Jugend, Information, (Multi-)Media ; Basisuntersuchung zum Medienumgang 12- bis 19jähriger.“ Zugriff am 12. Januar 2018. https://www.mpfs.de/fileadmin/files/Studien/JIM/2017/JIM_2017.pdf.
- . 2018. „JIM-Studie 2018: Jugend, Information, (Multi-)Media ; Basisuntersuchung zum Medienumgang 12- bis 19jähriger.“ Zugriff am 7. Februar 2019. https://www.mpfs.de/fileadmin/files/Studien/JIM/2018/Studie/JIM_2018_Gesamt.pdf.
- . 2020. „JIM-Studie 2020: Jugend, Information, (Multi-)Media ; Basisuntersuchung zum Medienumgang 12- bis 19jähriger.“ Zugriff am 9. April 2021. https://www.mpfs.de/fileadmin/files/Studien/JIM/2020/JIM-Studie-2020_Web_final.pdf.
- Murmann, Jule und Isabel Zorn. 2021. „Messenger-Dienste als Kommunikations- und Vermittlungstool in der beruflichen Bildung. Am Beispiel des Einsatzes von Threema in der Umschulung zu Kaufleuten für Büromanagement am BFW Köln.“ <https://idit.online/publikationen>.
- Nebel, Maxi. 21.22.2019. „Digitales Lernen – Datenschutzrechtliche Beurteilung von Lernplattformen.“ Forum Privatheit Jahreskonferenz 2019: „Aufwachsen in überwachten Umgebungen – Wie lässt sich Datenschutz in Schule und Kinderzimmer umsetzen?“, Berlin, 21.22.2019. Zugriff am 3. April 2020. https://www.forum-privatheit.de/wp-content/uploads/Nebel_Digitales-Lernen_Datenschutzrecht-bei-Lernplattformen.pdf.
- . 2021. „Digitales Lernen – Datenschutzrechtliche Rechtsgrundlagen von Lernplattformen für Kinder und Erwachsene.“ In *Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend*, hg. v. Ingrid Stapf, Regina Ammicht Quinn, Michael Friedewald, Jessica Heesen und Nicole Krämer. 1. Auflage, i.d.B. Reihe Kommunikations- und Medienethik. Baden-Baden: Nomos.

- Neß, Karsten. o.J. „Privacy Handbuch: Messenger.“ Zugriff am 26. Juni 2020. https://www.privacy-handbuch.de/handbuch_74.htm.
- Oliveira, Domingos de. 2016. Barrierefreiheit im Web 2.0: Ein Leitfaden zu Behinderung und Social Media. Norderstedt: Books on Demand.
- Pavkovic, Aleksander. 2021. E-Mail, 8. März.
- Pehl, Manuel und Christoph Knödler. 2020. Datenschutz und Schweigepflicht in der Sozialen Arbeit: Erläuterungen und Schaubilder für Ausbildung und Praxis. 1. Auflage. Regensburg: Walhalla Digital.
- Reece, Andrew G. und Christopher M. Danforth. 2017. „Instagram photos reveal predictive markers of depression.“ *EPJ Data Science* 6:1–15. doi:10.1140/epjds/s13688-017-0110-z.
- Reh@pp-Quality. 2016. „App-QKK. App-Qualitätskriterienkatalog.“ Zugriff am 13. Juni 2020. <http://www.rehatechnologie.fk13.tu-dortmund.de/rehapp/Medienpool/Dateien-zum-Download/App-QKK.pdf>.
- Schmid, Ulrich, Lutz Goertz, Julia Behrens und Bertelsmann Stiftung. 2016. „Monitor Digitale Bildung: Berufliche Ausbildung im digitalen Zeitalter.“ Unveröffentlichtes Manuskript, zuletzt geprüft am 7. Januar 2019. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Studie_Monitor-Digitale-Bildung_Berufliche-Ausbildung-im-digitalen-Zeitalter_IFT_2016.pdf .
- Schönenberger, Erik. 2016. „WhatsApp, E-Mail, SMS & Co. auf Sicherheit und Nachhaltigkeit bewertet.“ Zugriff am 26. Juni 2020. <https://www.digitale-gesellschaft.ch/2016/11/07/whatsapp-e-mail-sms-co-auf-sicherheit-und-nachhaltigkeit-bewertet-produktvergleich/>.
- Schulz, Ann C. S. und Sozialforschungsstelle TU Dortmund. 2019. Ausbildung zur digitalen Teilhabe? Eine Analyse der Lehrangebote zu Medienkompetenz in sozialen und pädagogischen Studienfächern an deutschen Hochschulen | Beiträge aus der Forschung Band 202 202. Dortmund: Sozialforschungsstelle TU Dortmund. Zugriff am 6. September 2019.
- Siller, Friederike, Angela Tillmann und Isabel Zorn. 2020. „Medienkompetenz und medienpädagogische Kompetenz in der Sozialen Arbeit.“ In Kutscher et al., *Handbuch Soziale Arbeit und Digitalisierung*, 314-332.
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin. 2005. „Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung Studie im Auftrag des Bundesministeriums für Bildung und Forschung.“ Unveröffentlichtes Manuskript. https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf.

- Verbraucherzentrale. 2018. „Datenschutzregeln bei Messengern mit Verschlüsselung im Überblick.“
https://www.verbraucherzentrale.de/sites/default/files/migration_files/media243857A.pdf.
- . 2020. „WhatsApp-Alternativen: Messenger im Überblick | Verbraucherzentrale.de.“ Zugriff am 15. September 2020.
<https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055>.
- Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0). BITV 2.0. Bundesministerium der Justiz und für Verbraucherschutz. 12. September 2011. https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html.
- Werz, Daniel. 2019. „Jabber (XMPP+OMEMO) statt WhatsApp & Co.“ Zugriff am 9. April 2021. <https://werznet.de/xmpp.html>.
- Wikipedia. 2020. „Liste von mobilen Instant-Messengern – Wikipedia.“ Zugriff am 13. Juni 2020. https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern.
- Williams, Marc. o.J. „Secure Messaging Apps Comparison | Privacy Matters.“ Zugriff am 13. Juni 2020. <https://www.securemessagingapps.com/>.
- Zehe, Marcos. 2018. „Alternativen zu Google & Co. Barrierefreiheit ein wichtiger Faktor - Marcos Leben.“ Zugriff am 9. April 2021. <https://www.marcos-leben.de/alternativen-zu-google-co-barrierefreiheit-ein-wichtiger-faktor/>.
- ZEIT ONLINE. 2019. „Datenschutz: Liest Google meine E-Mails mit?“. Zugriff am 27. Januar 2021. <https://www.zeit.de/digital/2019-08/datenschutz-unternehmen-e-mails-sicherheit-google>.
- Zorn, Isabel, Jule Murmann und Asmae Harrach-Lasfaghi. 2021a. „Kriterien für die Auswahl Privatsphäre schützender Messenger für Einrichtungen der Sozialen Arbeit.“ In Stapf et al., *Aufwachsen in überwachten Umgebungen*, 331–49.
- . 2021b. „Recherche DSGVO-konforme Messenger-Apps für Bildungseinrichtungen. 3. Auflage.“
https://idit.online/fileadmin/user_upload/Working_Paper/Datenschutz_und_Barrierearmut_bei_Messengerdienste_fuer_Bildungseinrichtungen.xlsx.
- Zorn, Isabel, Angela Tillmann und Winfred Kaminski. 2014. „Medienpädagogische Grundbildung in den Studiengängen der Fakultät für Angewandte Sozialwissenschaften an der Fachhochschule Köln.“ In *Grundbildung Medien in pädagogischen Studiengängen*, hg. v. Peter Imort und Horst Niesyto, 167–79. München: kopaed.

IV Anhang: Websites der Messenger-Anbieter

Chiffry; <https://www.chiffry.de/faq/>
Discord; <https://discordapp.com/>
Hoccer; <https://hoccer.com/>
Mattermost; <https://mattermost.com>
Ownchat; <https://www.ownchat.de/>
Schoolfox; <https://schoolfox.com/>
Schul.Cloud; <https://schul.cloud/>
Sid; <https://sid.co/de/>
Signal; <https://signal.org/>
Teams; <https://docs.microsoft.com/de-de/MicrosoftTeams/>
Telegram; <https://telegram.org/>
Threema; <https://threema.ch/en>
Wire; <https://wire.com/en/>

Verschiedene XMPP-Clients:

<https://blabber.im/>
<https://f-droid.org/en/packages/eu.siacs.conversations>
<https://atalk.sytes.net/atalk>
<https://monal.im/>
<https://siskin.im/>
<https://gajim.org/>