Isabel Zorn | Jule Murmann | Asmae Harrach-Lasfaghi

Data Protection and Accessibility in Digital Communication - Criteria for the Selection of Messenger Apps for Educational Institutions

Working Paper No. 6 of the project
IDiT - Including.Digital.Twins

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

ESF
Europäischer Sozialfonds
für Deutschland

Europäische
Union

Zusammen.
Zukunft.
Gestalten.

Imprint

Authors: Isabel Zorn, Jule Murmann, Asmae Harrach-Lasfaghi
Cologne University of Technology
Institute for Media Research and Media Education
Faculty of Applied Social Sciences
Gustav-Heinemann-Ufer 54
D-50968 Köln
Germany

Contact:
Prof. Dr. Isabel Zorn
isabel.zorn@th-koeln.de
Website: https://idit.online/

Cologne, April 2021

This working paper is an English translation of
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_Aufl1.pdf

Suggested Citation:
Zorn, Isabel; Murmann, Jule; Harrach-Lasfaghi, Asmae (2021): Data Protection and Accessibility in Digital Communication - Criteria for the Selection of Messenger Apps for Educational Institutions. Ed. by TH Köln University of Applied Sciences. Cologne (Working Papers IDiT, No. 6). Available online at https://idit.online/fileadmin/user_upload/Working_Paper/Messenger_Criteria_Education_IDiT_WP6_Ed1.pdf

Source credits of the image used on the title page: Niederrhein University of Applied Sciences - stock.adobe.com
Use of logos under trademark law

The project underlying this publication, "IDiT - Including.Digital.Twins. Inclusive mentoring and media skills for rehabilitation students and trainees in commercial professions/vocational training" was funded by the German Federal Ministry of Education and Research and the European Social Fund under the funding code 01PE18015B from 2018 to 2021 as part of the funding program „Inklusion durch digitale Medien in der beruflichen Bildung". It was carried out by the TH Köln, the Hochschule Niederrhein and the Berufsförderungswerk Köln (management).

The goal of the European Union is to ensure that all people have a career perspective. The European Social Fund (ESF) improves employment opportunities, supports people through training and qualification and helps to reduce disadvantages in the labor market. More about the ESF at: www.esf.de.

Table of contents

I Abstract

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 and privacy-preserving support of educational processes through software (Karaboga et al 2014; Digitalcourage e.V. n.d.) , as well as for 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 Introduction

In an increasingly digitized communicating society, educational institutions are also challenged to make decisions about whether and how they communicate digitally with their addressees. Because of their prevalence and frequent use by addressees and their useful features, messenger apps are increasingly being used in an unplanned way, at least among the addressees themselves. For example, students are increasingly using WhatsApp to communicate privately with each other about school-related content. (Medienpädagogischer Forschungsverbund Südwest 2018) . It is also common to observe that individual dedicated employees in institutions communicate with colleagues or addressees on their official or private cell phones via WhatsApp with the intention of improving a process and thus consciously or unconsciously commit legal violations.

Such privately organized communication channels demonstrate the need, but are often not data-protective. Decisions by institutions on whether and which software or apps (i.F. software) to use require sufficiently secure information as a basis on what to look out for in the selection process. Up to now, the information situation has been thin. On the one hand, there is not enough meaningful and comparable data on the individual software products. There are various criteria tables for free messenger apps, some of which are detailed. (Wikipedia 2020; Verbraucherzentrale 2018; Williams o.J.; Digitalcourage e.V. o.J.; Cryptoparty 2019; Verbraucherzentrale 2020; Initiative Freie Messenger 2020b). . However, these can usually only serve as information for private decisions by individuals, as there are more comprehensive legal requirements and context-specific goals for use by educational and social work organizations.

Second, educational institutions often need systematized requirement criteria. Scientific literature on the requirements of such institutions for internal and external communication to fulfill their educational tasks hardly exists: Which tasks should and must be supported by messenger communication? Which features can be disruptive or helpful for this purpose? What needs to be taken into account when it comes to the inclusion of all possible users? Which topics or contexts require or prohibit the use of messengers? What legal, ethical, and organizational consequences can messenger communication entail? How can the acceptance of messengers by the addressees be expected? The lack of information described above may explain why so few institutions have systematically used messengers to date. The need for appropriate information may be considered high if schools and youth institutions have so far provided little in this regard and their staff and addressees "google", "skype", "doodle" and "whatsapp" despite concerns about privacy (cf. mpfs 2018; D21 2017) and thus disclose sensitive data of sometimes vulnerable people. We have already described what to look out for when using messengers in social work contexts (Zorn, Murmann, and Harrach-Lasfaghi 2021a). .

This article aims to systematically elicit the requirements of educational institutions for potential messenger communications, and thus contribute to the information base on whether and how privacy-preserving messenger software can be used in educational contexts to reach a broad vulnerable population.

The article therefore addresses the question:

What criteria must and can educational institutions use when selecting messenger software?

It also explains why these criteria are important in educational institutions. The results are briefly outlined. The test results and characteristic values of the individual messenger apps are described in the results table cited several times here (Zorn, Murmann, and Harrach-Lasfaghi 2021b). .

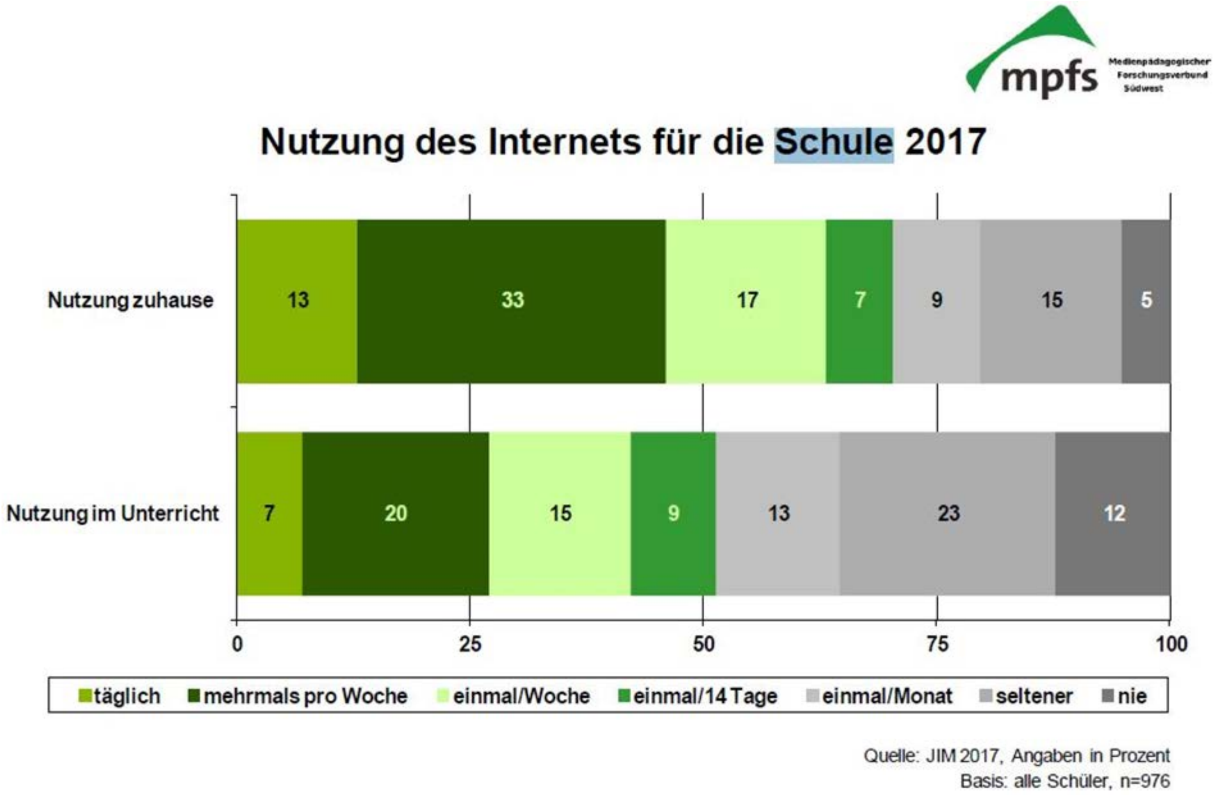
2 Digital communication in educational institutions

2.1 Growing digital communication needs in educational institutions

Almost all teenage students own a smartphone (mpfs 2019). The small mobile computers can be of great use for communication with each other but possibly also with teachers. These include school organization, information exchange, collaborative learning via messenger (cf. Pölert 2018), but also informal exchange. Examples of communication needs that can be implemented with messengers are:

- Debriefing tasks
- Mutual clarification of questions regarding homework or before class tests
- Task submission to missing students, e.g. students who are ill.
- Queries for appointments
- Reminders of times and meeting places or directions for excursions
- Queries to all parents
- Agreements among the teachers
- Task transfer and organizational arrangements in distance learning
- Informal exchange

One might object that all this is possible without Messenger, but more than half of children and young people state that they can no longer imagine organizing school without a smartphone, according to the results of the JIM studies. WhatsApp, Youtube and GoogleDocs are enjoying increasing use by learners (Medienpädagogischer Forschungsverbund Südwest 2017; Schmid et al. 2016) . 87% of young people use a WhatsApp group for school classes (Medienpädagogischer Forschungsverbund Südwest 2020, 39)



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

Fig. 1: Use of the Internet for the school

According to a study by the Bertelsmann Foundation on the digitization of vocational education and training (Schmid et al 2016: p. 27), only 7% of teachers at vocational schools use messengers for their day-to-day work at the vocational school, while 18% of trainers use "communication applications, e.g. WhatsApp, Skype" (loc. cit.: p. 32). According to this, it can be seen that the participants look for their own solutions for digital communication if the schools or training companies do not provide suitable communication offers. However, this leaving of the choice risks that the selection of tools may not be decided along regulations regarding data protection or the inclusion of all students. It is likely that the most popular softwares will prevail regardless of their school-related suitability. In this regard, Lower Saxony plans to use the smartphone as a learning tool from 2021 in its "Master Plan for Digitization". Privacy-compliant alternatives to WhatsApp, Dropbox, Google Drive, etc. (cf. Pölert 2018) are largely lacking, however. Even under the so-called Corona crisis, the need for digitally supported teaching with secure email addresses, messengers and filesharing options became apparent. It has been true for some time that adolescents understand peer pressure to use WhatsApp as a "duty" (Gebel, Schubert, and Wagner 2015). Experience shows that it is common for learners in many educational institutions to organize themselves in their classes or courses of study through WhatsApp groups.

2.2 Risks and problems of the use of messengers in school or socio-pedagogical contexts

In order to show what the problems are when the given needs for digital communication tools are satisfied by the participants through their own solutions, aspects of data protection, privacy, exclusion and media competence are explained below.

Schools and educational institutions such as the Berufsförderungswerke train people of great diversity, including those who tend to belong to more disadvantaged, vulnerable groups. Often their financial situation, their living situation, their opportunities for participation are below average and they are at risk of further disadvantages. Therefore, the issues presented below, such as data protection and accessibility, are practice-relevant categories for the protection and current and future equal opportunities of learners.

2.2.1 Privacy

Personal data is collected by the providers of all of the software offers mentioned above as examples (WhatsApp, Youtube, GoogleDocs). However, according to the General Data Protection Regulation (GDPR), personal data may only be collected and, if necessary, processed and stored on the basis of specific legal grounds or with the effective consent of the persons concerned. For the personal data of students, teachers and guardians collected by schools as part of their educational mission, such a legal basis includes the school laws. These stipulate that personal data may only be collected, stored and processed internally and only for the regulated purposes. However, the aforementioned software transfers the collected data to company servers, where it is stored and processed. The data transfer often takes place invisibly in the background of the app, those who do not have detailed knowledge will often not notice them and unknowingly pass on data. WhatsApp regularly transfers the entire address book of a cell phone user to the company servers in the USA. WhatsApp collects a lot of information about users and their devices, including device ID and matches it with the device ID used for Facebook, for example (cf. https://www.whatsapp.com/legal/?l=de#privacy-policy).

WhatsApp reserves the right to pass on the data it receives to Facebook, where it can be linked to many details about the user, e.g. photos, preferences, interests, behavior, likes. (cf. https://faq.whatsapp.com/general/security-and-privacy/how-we-work-with-the-facebook-companies?eea=1 , analytically also Pehl/Knödler 2020).

If the app automatically sends personal data of the contact persons, a person who installs WhatsApp on the cell phone must first ask all persons whose data he or she has stored in his or her address book for permission to forward this data to WhatsApp. The so-called WhatsApp ruling reminds legal guardians of their duty of care in this regard (Buchner 2017); a lawsuit filed by the consumer advice center is pending under case number 52 O 22/17.

The use of WhatsApp for school purposes is therefore illegal under the Lower Saxony School Act, for example (Section 31 NSchG) (Landesbeauftragte für den Datenschutz Niedersachsen 2018). In Schleswig-Holstein, any Messenger use in schools is illegal. There are a variety of unresolved organizational questions under school law (LDB-SH 2016), including on the billing of communication between teachers and students and their parents. A very good reference point for this would be the already existing rules for handling and using e-mail, as there is an analogy between "chat" and "e-mail" (federal structures, same IT principles). The only additional things to consider are typical functions of instant messages such as "online status," "currently typing," and "last online.

Further links on digital offerings of the educational institutions that link to external offerings, such as to explanatory films on YouTube, are therefore only permitted under data protection law if the learners have been informed about this beforehand and have consented. Such links are often used on learning platforms or in chats on messengers in an indicative manner. However, consent may be required here.

To protect against legally questionable use of communication tools, many schools respond with bans, but these are difficult to enforce consistently. Moreover, they do not solve the problem, as the need for communication remains.

2.2.2 Privacy, Predictive Analytics and Exclusion

The current and future technical possibilities of collecting and processing seemingly unimportant data allow unexpected recognitions, inferences, and diagnoses of individuals. The analyses of the voice assistant system "Alexa" diagnose acute colds or mood swings (Jin and Wang 2017). For several years now, an algorithm has been able to diagnose depression by analyzing posted Instagram photos, more accurately than trained psychology professionals in the study control group (Reece and Danforth 2017). Future advanced analytics for behavioral prediction, e.g., about performance or susceptibility to illness, are expected.

Data from learners can be understood as particularly sensitive data if they allow conclusions to be drawn about, for example, diligence, perseverance, speed, peer networks, etc., and can be compared with each other or linked to other meaningful data. Particularly for disadvantaged individuals from vulnerable groups, these diagnoses and predictions are potentially disadvantageous if they are diagnosed or predicted to have low performance or if such data will increasingly be available for sale in the future. Thus, in particular, data from low-performing students who are at a sensitive developmental age are particularly worthy of protection for these additional reasons. In addition, the phenomena of digital inequality often apply to these people. For example, it is often educationally disadvantaged people who, in the wake of digital inequality (Bos et al. 2014; Klein and Pulver 2019; Iske and Kutscher 2020; Initiative D21 e.V. 2018, 24), also have less knowledge in the confident, data-protective use of digital tools. This may involve, for example, securing profiles and personal data or controlling cookie settings and app permissions, and many more. It is conceivable that the algorithmically generated predictions about people will be sold in the form of data and profiles and may, for example, lead to further disadvantages and fewer opportunities for participation in health insurance schemes, application procedures, and insurance benefits.

For example, efforts to include people currently in educational contexts, including by means of digital communication tools, without taking their risks into account, can lead to people being at risk of disadvantage or exclusion in the future because of the data collected in these measures.

2.2.3 Media literacy and digital competence

As long as there is a demand and attractive free software that is problematic in terms of data protection promises to satisfy it, bans without the simultaneous provision of a suitable alternative are unlikely to be effective. The task and challenge for educational institutions is also to develop and promote the media competence of learners, to familiarize them with the possibilities and risks as well as the background of dealing with digital media, and here, for example, also with diverse and also suitable messenger offers. This requires media competence and media pedagogical skills on the part of the professionals. However, the teaching of media pedagogical competence in education in pedagogical courses of study or those for social work is marginal (Schulz and Sozialforschungsstelle TU Dortmund 2019; Imort and Niesyto 2014; Zorn, Tillmann and Kaminski 2014). Media literacy in the adult population can also still be described as low in some cases (Initiative D21 e.V. 2018, 21ff). A model for the development of media pedagogical competence for professionals is available and states that in particular the identification of suitable media in the field of action should be performed according to all specifications to be considered (Siller, Tillmann and Zorn 2020).

However, the perspective on the development of media pedagogical competence among professionals is not sufficient: Even if competence exists, the research

preceding a decision is so time-consuming that it can hardly be expected of individual professionals. The research situation regarding the requirements to be fulfilled as well as the fulfillment of these requirements by various software is non-transparent, the information situation is thin. The research within the studies we conducted revealed a great lack of clarity about what teachers, social workers may and should use. This lack of clarity and support in the selection process can lead to no or inappropriate usage decisions. The complexity of a media selection process was exemplified in the spring of 2020 under COVID-19 prevention efforts, when even higher education institutions experienced ambiguity in selecting GDPR-compliant communications software due to sometimes insufficient information from software vendors, such as the video conferencing tool provider Zoom. Due to the urgent search of social youth institutions for digital communication tools, recommendations were made for software in youth institutions that are clearly not GDPR compliant (https://www.jugendleiter-blog.de/corona/ and https://www.offene-jugendarbeit.net/index.php/okja-in-corona-zeiten/okja-in-coronazeiten).
This explains why, despite the GDPR and state school laws, software and apps that can be classified as critical, such as WhatsApp, are still used in schools and social institutions (e.g. for class chat, street work, residential groups).
A reference to media competence among professionals as an explanation therefore falls short (Zorn 2017).

Recommendable introductory information portals on secure software in general exist, e.g.

-Digitalcourage: https://digitalcourage.de/digitale-selbstverteidigung

-Klicksafe: http://www.klicksafe.de

-Me and my shadow: https://myshadow.org/resources (will no longer be updated)

-Do not Track: https://donottrack-doc.com/de/episodes

-Internet ABC: https://www.internet-abc.de

-Irights.info: https://irights.info

In addition, meaningful criteria checks for the security of messengers exist for private use (Schönenberger 2016; Incobs 2015; Kuketz 2020; Williams o.J.; Wikipedia 2020; Neß o.J.; Initiative Freie Messenger 2020b).
The problem with these existing information portals on safe software, however, is that while they provide statements about individual safe use, they do not provide meaningful enough information for decisions about institutionalized use.

3 Method of the study for the selection of messenger software in vocational training

Various messenger offerings were examined according to criteria. The focus of the study was to explore the risks and opportunities for using messenger in vocational training and to develop and systematically present the relevant criteria. Possible apps were researched, categorized and theoretically assessed. Messenger apps that could be used in an educational context were also tested in practice. Subsequently, a decision was to be made as to whether and, if so, which messenger could be used in the IDiT project in the Berufsförderungswerk and in other vocational training contexts. The considerations of this selection process based on the criteria developed are described in Chapter 6.

3.1 Survey of the requirements for a fair use in educational institutions

The permissions, restrictions and requirements to be taken into account for the use of communications software in educational institutions were to be systematized. For this purpose, extensive literature was researched, e.g., the requirements by law as well as by state data protection officers. In addition, due to the topicality of the topic and the limited amount of published research on the subject, Internet-based reports, commentaries, and questions and answers to data protection experts were researched. Due to the limited availability of meaningful printed literature on the topic, experts were consulted in the form of ad hoc telephone calls/email inquiries (data protection officers, social work employees, teachers). Methodologically, detailed evaluations of the surveys will not be made here. The suggestions of the interviewees were used as a starting point for our own research. From this, we created a systematic and reasoned presentation of the specific requirements of educational institutions.

The results are presented in chapter 4.

3.2 Creation of test criteria

For an informed analysis of messengers and the presentation of their characteristics relevant to educational institutions, the legal and practical bases had to be determined from the requirements presented and, in particular, criteria had to be developed from them according to which messengers can be described, compared and their suitability for specific contexts determined.
We defined the necessary criteria with the help of the developed requirements based on findings from the expert survey, the table evaluation, and the literature and legal research. To this end, we researched existing criteria tables for assessing messenger apps (Wikipedia 2020; Verbraucherzentrale 2018; Williams o.J.; Digitalcourage e.V. o.J.; Cryptoparty 2019; Verbraucherzentrale 2020; Initiative Freie Messenger 2020b) and used criteria for assessing the accessibility of apps in general (Bundesministerium der Justiz und für Verbraucherschutz 2011; Oliveira 2016; Aktion Mensch and Stiftung Digitale Chancen 2010; Reh@pp-Quality 2016).

We examined the criteria used there and compared them with the requirements for educational institutions. As a result, we adopted parts of the test criteria used there. It became apparent that the criteria usually used were sufficient to check compliance with the GDPR, but not sufficient to check accessibility and practicability. In addition, some of the test criteria were formulated in a very technical way, and we provide an explanation of their meaning and relevance for the educational context. For the insufficient tests, we developed our own test criteria for the context of inclusive vocational education and explained them.

In addition, we tested those individually available messenger apps that met the data protection requirements after thorough examination. On the basis of the tests, we discovered and developed further test criteria for the practicability of an app, because it was only through practical testing that it became clear where practical differences between individual apps could lie. This concerned, for example, necessary requirements or procedures for the installation, for the integration of contacts, for the backup of data and others. Such information is often missing from the manufacturer's information on their websites; for example, it is not always specified which data is necessary when starting up the app (e.g. phone number? e-mail address? SIM card necessary?).
The model of the developed test criteria is presented in Chapter 5.

3.3 Selection of messenger apps to be reviewed

After the development of criteria for the conditions of use of messenger software, the offer of the multitude of available messengers should be sifted and systematized. Existing lists of available messengers were reviewed. It became apparent that the lists are incomplete, e.g. Ginlo or Quicksy are missing from the extensive Wikipedia list (Wikipedia 2020).
A selection was made from the pool of available messenger apps. Apps and messenger systems were selected for closer examination,

1. which are very popular and widespread and/or
2. that are German-based or Europe-based and suggested compliance with GDPR.

Extensive background information was researched for the selected apps, and in some cases we made phone calls to the providers to obtain the necessary information because they are not listed in freely available provider sites or independent criteria tables. We checked the information on the latter because of the fast pace of developments on the provider sites.

The research led us to systematize the multitude of messenger offers:

We divided apps into 3 groups:

A) **Provider-dependent** (proprietary) messengers available to **individuals/private parties;**

1: Signal, WhatsApp, Telegram, Discord.

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

B) **Provider-independent** ("free") and international standard (XMPP) based apps available to individuals/private[1] parties ;

for Android: Conversations, blabber.im (formerly "Pix-Art"), Quicksy.

for iOS: Siskin, Monal, ZOM, ChatSecure, JabMe.

C) **Apps to be purchased by companies or institutions** to be made available for institutional communication.

The range of institutional solutions is large. Our selection was arbitrary in that the focus in the IDiT project was not initially on selecting an institutional app). However, such apps were to be included in the study in order to use them as examples to demonstrate the possibilities and limitations of enterprise solutions: school.cloud, SchoolFox, OwnChat. This also includes the enterprise solution Threema Work, which was later selected for the IDiT project. One of the apps presented should be based on open source software to show the possibility of hosting your own with free software: Mattermost.

[1] With current knowledge, apps based on the Matrix protocol also seem promising as "free" (provider-independent) apps, e.g. Element (Initiative Freie Messenger o.J.c).

The aim of the further testing of the apps was to find a suitable messenger available for private individuals for the voluntary use of learners in vocational education in the inclusive project IDiT. This stemmed from the idea and the desire to simultaneously expand the learners' media literacy and messenger skills in the dimension of their media literacy with the selection and use of a messenger app in the educational context and to let them gain experience with a messenger app that they could also use in their private lives as a GDPR-compliant app. In this respect, we focused on apps that do not have to be provided by the educational organization as an internal organizational app (see Chapter 7).

3.4 Audit according to data protection requirements

In the next step, the selected messenger apps were analyzed using the test criteria developed for data privacy. Their characteristic values for the individual criteria were researched and recorded in the results table. To obtain information about a feature of an app, other comparison sites (Wikipedia 2020; Verbraucherzentrale 2018; Williams o.J.; Digitalcourage e.V. o.J.; Cryptoparty 2019; Verbraucherzentrale 2020; Initiative Freie Messenger 2020b) were also consulted to obtain indications of the characteristics of an app, but all features were searched for and documented on the app's provider pages. One problem is that these characteristics of an app can change quickly in the course of rapid development cycles. In this respect, it is important to note that the documented data applies to the period from January to September 2020.
The results can be found in table form in the published results table (https://idit.online/publikationen). The external comparison tables used are also listed there in the literature list.

3.5 Testing for features and practicality

This test followed the same procedure as the test for data protection requirements. The characteristic values for the developed practicability criteria were researched for the entire sample. In addition, the GDPR-compliant, individually usable apps were tried out (unsystematically) on various devices: they were installed on one newer and one older iOS smartphone and Android smartphone respectively, put into operation, a chat account was created, contacts were integrated, and various messages and media were sent to each other and audio and video calls were made. The findings on the available features and the practicality of the applications were recorded in tabular form in keywords or in characteristic values.

4 Results I: Special requirements for messenger communication in educational institutions

The special requirements in educational institutions are outlined below as a basis for developing suitable criteria. These requirements form the basis for the criteria to be developed when analyzing messenger apps for their potential suitability for use in educational institutions.

4.1 Data protection/personal data

There are different regulations in the federal states as to whether and how software may be used in educational institutions. In the case of ecclesiastical institutions such as BFW Cologne, there are also special ecclesiastical data protection laws. In principle - in accordance with the GDPR - the protection of data relating to individuals must be observed. However, the form of protection may be regulated differently, for example, whether work with personal data is fundamentally restricted to certain devices (only service computers, no smartphones).

It follows from their mandate that vocational training centers in particular deal primarily with vulnerable groups and therefore with particularly sensitive data, because even admission to vocational training in a vocational training center is linked to certain diagnoses or characteristics of disadvantage. In fulfilling their tasks, the facilities must therefore comply with the requirements of the associations and sponsors, for example, and in some cases also see themselves as bound by certain ethical imperatives, such as the ethics of the DBSH professional association. (Deutscher Berufsverband für Soziale Arbeit e.V. 2014) , are obligatory.

4.2 School Laws

The question of the use of messenger services in the school and training context is governed not only by the usual rules of compliance with telecommunications law regulations, but also by more far-reaching questions of school law. These include questions about the binding nature of the communication in terms of content and law, or whether the communication is secure and whether the official communication data may be processed (stored) securely and technically separately from private communication data on the teachers' private end devices. However, this aspect could be countered by the use of official devices or by the use of messenger services that only work on a computer even without a smartphone. Practical issues relevant to school law are: For example, if teachers at a school want to systematically distribute classroom materials or homework to students exclusively through a messenger: Can the school require that all students in a class actually own a terminal device (smartphone, tablet or computer)? Can the school mandate that a smartphone must be present and used for classroom management? Is it legally possible to prescribe a certain service (possibly with costs)? Under what conditions?

4.3 Communication with authorities

Schools and social work agencies often need to communicate with authorities about legal aspects of their protégés. In this respect, communication with protégés can become legally relevant. This raises questions about the possibilities of verifying this communication - what is easily possible with e-mail through printouts must be examined with messenger software. Likewise, it must be clarified which personal data should and may be processed by which entities for which purposes, and whether personal information received or sent with the messenger could have file relevance, in which case end-to-end encryption may be undesirable in some cases because third parties (besides the two communicating parties) cannot view it. In such cases, normal transport encryption of the data must suffice. For letter and e-mail communication, schools in e.g. Schleswig-Holstein - as probably in all public bodies in Germany - have clear regulations on which processes are to be stored in pupil files.

Public bodies are obliged to prove the lawfulness of their (administrative) actions at all times to the person or persons concerned and, if necessary, to supervisory bodies such as the courts. The obligation to provide evidence in connection with personal data processing also arises from the requirements of the GDPR and, specifically in the school sector, from the provisions of the School Act and the School Data Protection Ordinance. Furthermore, questions arise regarding the deletion of data stored in a messenger on teachers' private devices. In Schleswig-Holstein, regulations exist in the School Act and the School Data Protection Ordinance for the deletion of personal data of students and parents. Furthermore, the Ministry of Education has issued instructions for handling and deleting e-mails.

When communicating in the context of schools and social work, it is important to consider whether confidentiality obligations apply and whether social data is transmitted. Legal requirements regarding secrecy, criminal confidentiality and social data protection in social work must be observed; this is regulated in particular in Section 203 (3), (4) sentence 2 no. 1 of the German Criminal Code (StGB) and in provisions of Section 80 of the German Social Code (SGB X). There is a duty of confidentiality for the contents shared in the professional context.

4.4 Educational mission

Educational institutions have a core mission of imparting education. Given the conditions of digitization in society and changes in lifeworlds, this educational mission also includes teaching media literacy and thus dealing with secure digital communication. If these educational institutions for messenger communication - which according to the JIM Study 2020 is the most active Internet activity of 93% of all young people (Media Education Research Network Southwest 2020) - they are not only ignoring communication needs, but also their educational mandate: Where are young people and people in vocational training supposed to acquire skills in these important areas, if not in their educational institutions?

4.5 Inclusion

In addition, educational institutions have inclusion as a duty and mandate; here, the UN Convention on the Rights of Persons with Disabilities with Articles 9, 21, 22, 24 should be mentioned in particular, which refer to accessibility to all information and ICT technologies as well as to education in order to enable equal participation in all social processes. In this respect, accessibility and barrier-free accessibility must be taken into account when selecting messenger software so that no one is structurally excluded from information processes. The knowledge and equipment of the learners can be very heterogeneous. Different operating systems are used, sometimes in old versions. Operating and user skills vary greatly, and attention must be paid to reading and spelling deficiencies or even illiteracy. The age of the users is also heterogeneous; in schools, it is usually under 16, but in vocational institutions, it can usually be assumed to be over 16. The minimum age of 16 makes it possible to decide independently on certain consents when using apps.

4.6 Obligation versus voluntary use

Where the appropriate legal foundations (e.g., school law) have been created (Nebel 2021, 21.22.2019) , an obligation to use digital tools in vocational education can be made possible. If these are not in place, voluntariness applies:
It must be possible to use additional digital services that are not part of the educational institution's required regular services voluntarily and without the threat of disadvantages. Examination-relevant content may not be conveyed exclusively via such services. The conditions under which the use of a terminal device (smartphone, tablet or computer) and a specific messenger can be made compulsory at school are still an unresolved issue under school law (see 3.2). Obtaining consent is to be avoided from a legal point of view (Nebel 21.22.2019) . In the case of provider-

independent messenger systems, users can choose which program/app they want to use.

5 Results II: Criteria for the selection of software in educational institutions

New software to be deployed in educational institutions must meet the above-mentioned relevant requirements. To this end, the legal and practical principles relevant to the planning of a software deployment must be determined in addition to the requirements. Based on these principles, criteria were developed in the next step according to which software - in this case individual messenger apps - can be tested. In summary, criteria for messenger selection need to be developed for three categories:

a) Data protection and privacy;

b) Accessibility and inclusion;

c) Practicability of use in institutions.

5.1 Data protection, privacy

5.1.1 Basics

The bases for the criteria development are:

(1) General Data Protection Regulation (DSGVO)

(2) School Law

(3) Legal requirements regarding confidentiality, criminal confidentiality and social data protection

Re 1: Compliance with the guidelines of the General Data Protection Regulation (European Parliament 2016) is a basic requirement for the selection of software in all institutional settings (while private individuals can choose not to exercise their right to privacy). Conventional check tables help to make exclusions of messengers in the selection process.

The GDPR determines how personal data may be processed by regulating principles (Art. 5 GDPR) and lawfulness (Art. 6 GDPR) of the processing of personal data. This includes, for example, whether the processing of one's telephone number and e-mail address requires consent. If it requires consent, app use in Germany is only permitted from the age of 16, or parental consent is required (Art.8 GDPR).

An essential criterion for GDPR compliance is the question of whether and which personal data is collected and further processed. The question of how a software handles contact data from smartphone address books and whether this contact data is stored and processed by the software provider is therefore particularly sensitive.

Re 2: School law in each federal state regulates the rights and obligations and the goals underlying learning and teaching in the state. This includes, among other things, how it is regulated which media and teaching materials and which teaching and learning systems can be used in schools (e.g. § 1 para. 6 SchulG RLP). In the course of this, it is also regulated whether a new introduction of a digital form of communication and learning (for example, via a messenger) is possible and whether the use is mandatory or only voluntary and how to proceed with the transmission of data to third parties (e.g., § 67 para. 6 SchulG RLP). The School Act also regulates which data employees such as teachers or school social workers may collect, store or share, or pass on to third parties (for an overview as a handout for teachers, see Independent State Center for Data Protection Schleswig-Holstein and Institute for Information Systems at Humboldt University Berlin 2005). Since names and contacts as well as content are potentially shared when using a messenger app, the requirements under school law must be placed in a context with the technical possibilities of a messenger app.

Test criteria can be: Is transfer to a file possible? Is computer use possible? Is use necessary or voluntary?

Re 3: Legal requirements regarding secrecy, criminal confidentiality and social data protection in social work, which also applies to school social work, for example, must be observed; this is regulated in particular in § 203 Para. 3, 4 Sentence 2 No. 1 of the German Criminal Code (StGB) as well as in provisions of § 80 of the German Social

Code (SGB X). There is a duty of confidentiality for the contents shared in the professional context.

5.1.2 Developed criteria for handling data protection and privacy

In accordance with the requirements for educational institutions, we developed the following test criteria. For this purpose, we used the general comparison tables mentioned in the methods chapter, whose criteria we adopted and supplemented according to the above requirements. This process required, in part, an assessment of technical characteristics as well as their practical relevance in educational contexts. (What relevance does it have for data privacy in an educational institution whether a messenger is open source and thus verifiable, whether it is chargeable, how much metadata is generated, whether the server is located in the EU or in Germany, whether the address book is sent, whether all communication or only parts of it is encrypted end-to-end)?

As a result, we developed the following testing criteria for messenger apps for testing the protection of transmitted data in educational institutions:

1. Overall impression according to the European General Data Protection Regulation: Compliant according to Art. 5 and 6 GDPR?
2. Service location
3. Service infrastructure
4. Consent: Age restriction (Art. 8 GDPR): Messenger apps that require the disclosure of personal data for registration are subject to an age restriction of 16 years according to Art. 8 GDPR. Otherwise, the consent of a parent or guardian is required.
5. Registration and commissioning: Is personal data, e.g. telephone number, e-mail, real name, etc., necessary for registration?
6. Is user data and/or meta data stored? (Principle of data economy) (Metadata: Who is online when; with how many and which devices someone is online; which contacts someone has. A great many conclusions about a person can

be drawn from metadata, e.g.: Who communicates (or doesn't communicate) with whom and when; who participates in which groups.

7. IP addresses of the devices
8. Store and Forward: Partial data transmission method in which information is sent via an intermediate station (e.g., a router), which stores the data and forwards it to the final destination or another intermediate station at a later time.
9. Data transfer: Does the app protect my messages and attachments?
10. Principle of accessibility and openness: Is the privacy statement available in German?
11. Address book: What happens to contacts from the address book? Are the contact data uploaded to the provider's server and stored and processed there in a readable form?
12. End-to-end encryption: A readable piece of information (plain text) is converted by a key into a text that cannot be read without this key. This ensures that decryption can only take place on the end devices of the users involved (and not on the transport route of the message and not on the provider's server).
13. Encryption & data security: Which cryptographic method is used?
14. Principle of openness: Does the company provide a transparency report?
15. Auditability: It can be determined retroactively who processed which personal data when and in which way.
16. GDPR seal: This seal only has a marketing value, but can be a decision-making aid for users with little experience.
17. Location tracking: Does the app send its own location? Location data are personal data according to Art. 4 No. 1 s. 1 GDPR personal data. According to Art. 5 GDPR, the principle of data minimization applies. Location data may only be collected and processed with consent.
18. Open source: Is the source code open? Only if the source code is open can parts of the provider's data protection information be verified.

5.1.3 Results of the audit according to data protection

5.1.3.1 GDPR compliance of messenger apps

The criteria were researched the characteristics of the messenger apps of the groups A,B, C. From the group of individually usable provider-dependent messenger apps (group A), most popular, widespread apps are problematic in terms of their unencrypted transmission and processing of contacts from the address book (which actually requires permission from the contacts), their server location, and the collection and non-encryption of metadata. With the exception of Telegram, all apps offer end-to-end encryption of message content by default.

The following provider-dependent messenger apps available to individuals (Group A) can be considered compliant with the GDPR after applying the test criteria:

- Threema (only partially open source)
- Hoccer (currently no longer exists)
- Wire
- SID (only beta version available; details and information about the protocol and standards used, the encryption and the source code only announced; the download address of the Android app runs (as of 02/2021) to nowhere)
- Ginlo
- Chiffry

For the assessment of the principle usability of Threema in social work according to GDPR conformity, there is also a current explicit legal consideration (Pehl and Knödler 2020) .

In addition, there is also the possibility of provider-independent apps that adhere to the international standard "XMPP" (Group B). A messenger app or program that speaks this protocol ("XMPP") is - unlike proprietary messenger apps - not tied to a central server provider. This is why such apps are called "free" messengers or provider-independent messengers. With these, the services of various server providers can be used, or contract or self-hosting is also possible. Whether server operators handle the collection, processing, and storage of data and metadata in a GDPR-compliant manner cannot therefore be traced back to the app itself. In this respect, both GDPR-compliant and non-GDRP-compliant server operators can be used with these messengers. A check of the criteria cannot only be carried out on the basis of the app used, but also depends on the server operator (as is also the case with e-mail). There must be a contract for commissioned data processing with this. However, the potential for this exists due to the apps: Address book entries are not automatically forwarded, and on mobile devices the apps work even without consent to access the address book. Almost all apps can be used without providing a phone number or e-mail address (exception: Android app "Quicksy," which is a special version of Conversations for a quick start on Android).

All messengers that forward address book entries unencrypted and store them on servers are not GDPR-compliant if it can be assumed that the contacts were not asked whether they agree to their data being forwarded to third parties (e.g. companies and servers). Depending on the operating system, this also includes widespread apps such as WhatsApp, Telegram, Facebook Messenger, Skype, Viber, Discord, and many more.

This makes it clear that the widely used messengers do not fulfill the basic requirement for use. In this respect, the need to select messenger software that is not widely used applies to the context of use in question. Actually, the messenger system that can then be used with one or more messenger clients (app/PC program) would have to be selected. However, this weakens a previously strong argument for the use of messengers, namely to use a medium that learners use in everyday life anyway and already have installed on their device.

"Institution-internal" messengers (Group C) are among those potentially complying with the GDPR. Here, the educational institution concludes a contract with the software provider anyway. In this, an agreement on commissioned data processing can contractually secure the corresponding protection of the data. These include, for example, the "enterprise versions" of Threema, Wire, Chiffry, SchoolCloud, OwnChat, Mattermost, Microsoft Teams and others. However, unfortunately,

questions about data protection remain open in some cases and an exchange with contacts outside the organization (parents' associations, parents, authorities, other schools, friends, ...) is hardly possible with a closed system. This in turn limits the use in contrast to e-mail (federated system).
The app Signal, which is often considered to be very data-secure and is now quite widespread, was co-financed by the US government (https://de.wikipedia.org/wiki/Signal_(Messenger)) and the servers are located in the USA, not in the EU. This can be considered an exclusion criterion because Signal is not subject to the applicability of the GDPR. However, since Signal wants to ensure protection in accordance with the GDPR, it has submitted to the non-enforceable voluntary commitment with the help of the Privacy Shield. Criticism of this is the lack of enforceability and that access by foreign intelligence services is not regulated. In addition, the suitability of the Privacy Shield was overturned by a European court ruling in 2020.

Thus, it becomes clear that the choice of messengers for which the GDPR applies and which handle personal data accordingly is limited.

5.1.3.2 Necessity of concluding a commissioned processing agreement

If, in the context of communication in an educational institution, data is generated via a messenger that falls under the obligation of secrecy or confidentiality, it is necessary to check whether the messenger provider assumes and can ensure confidentiality. Legally, however, this can be a gray area. For example, all messenger providers also accumulate metadata (e.g., who communicated when with whom and for how long), which is quite meaningful. The duration of storage and the amount of metadata stored is relevant. Legal certainty can only be achieved by concluding a commissioned processing agreement in accordance with Section 28 of the GDPR. One criterion is therefore whether such an agreement can be concluded with the provider of the product. This is possible even with provider-independent chat. Here, there are commercial companies or registered associations that operate corresponding servers and ensure this. Servers provided to the general public by private individuals cannot fulfill this criterion. Practically and safely, this can also be made possible by concluding a contract for a paid version of a messenger, for example for enterprise/pro versions of messenger systems, i.e. internal organizational solutions. In most cases, even consumer and work versions of a messenger app are compatible and the need to purchase a pro version is only necessary for the professional specialists (for a detailed discussion of all legal tests: Pehl/Knödler 2020). The possibilities of a commissioned processing agreement are legally secure for an institution and thus advantageous, as they make any necessary consent according to Art. 6 or 8 GDPR of the users superfluous, which can always bring difficulties (withdrawal of consent, consent in case of power imbalances). Taking into account all the criteria listed here, if an educational institution needs to conclude a commissioned processing agreement, either the selection of an organization-internal messenger or the commissioned hosting or even self-hosting of a provider-independent system comes into question.

The focus of the present study to particularly examine messengers in the sample that are freely available to private individuals thus proved to be potentially problematic under the aspect of the possible need to conclude such an agreement. In the course of the research, it became apparent under the requirement for confidentiality mentioned under requirements that the requirements for using a messenger app in an educational context are high. If one wants to take all confidentiality and secrecy obligations into account, only apps with which the educational institution has concluded an agreement on commissioned processing come into question. However, if one considers that and how carelessly teachers and learners communicated via unencrypted commercial e-mail providers in many schools and educational institutions - especially increasingly during the COVID 19 prevention measures - the claim of an actual agreement on commissioned processing is revised: It seems that in many cases, communication in schools and educational institutions takes place via the learners' private e-mail addresses, and without encryption. Learners also often seem to be required to provide an email address to log into a school learning platform system (e.g., moodle). (exemplary: integrated comprehensive school Zell 2020) , homework was also sent via email. If no encryption takes place here, then all contents and names are present in clear version with the respective E-Mail offerers, who are often data evaluating offerers, usually also on foreign, often US-American servers, e.g. Gmail (ZEIT online 2019) , YahooMail, Hotmail, but also GMX mail analyzes, if necessary, the contents of emails in the "intelligent mailbox" (https://www.gmx.net/mail/intelligentes-postfach/). It is therefore questionable here whether, in contrast, the use of a GDPR-compliant freely available messenger that offers end-to-end encryption of all content is not more sensible - even without an agreement on commissioned data processing. Examples would be Threema, Wire, Chiffry, Ginlo (the latter three unfortunately with the need to provide personal data such as email address or phone number) and those provider-independent chat programs/apps that use a secure server.

5.2 Accessibility

5.2.1 Basics

The basis for the high relevance of the consideration of low barriers and thus the development of test criteria are:

1. UN Convention on the Rights of Persons with Disabilities (UN CRPD), Art. 9, 21, 22, 24, combined with requirements from the Social Codes on youth welfare (Social Code Book 8) and inclusion (Social Code Book 9)
2. Barrier-free Information Technology Ordinance (BITV) 2.0
3. Intuitive operation
4. Target group-specific needs (e.g. reading/writing/language difficulties)

Re 1 and 2: According to the ratified UN CRPD, digital information and information technologies must be accessible to all people: Art. 9 (1): "In order to enable persons with disabilities to live independently and to participate fully in all aspects of life, States Parties shall take appropriate measures with the aim of ensuring for persons with disabilities access on an equal basis with others to the physical environment, means of transportation, information and communication, including information and communication technologies and systems ...". From this it can be deduced that accessibility to all information and all information and communication technologies must also be guaranteed in schools and other educational institutions. In addition, educational opportunities as well as the forms of communication and means of communication used there must be usable for all people (cf.: Art. 24 (3, c): States Parties shall ensure "that education is provided to blind, deaf or deaf-blind persons, in particular children, in the languages and forms of communication and with the means of communication best suited to the individual"). Accordingly, the school use of a messenger app that cannot be used by blind students to communicate together, for example, could be interpreted as impermissible if that puts students at a disadvantage in education-related communication processes. The Barrier-Free Information Technology Ordinance (Barrierefreie-Informationstechnik-Verordnung, BITV) 2.0 makes further and concrete specifications in this regard, but so far it is not very specific for apps and rather makes specifications for websites. BITV 2.0 is intended to ensure comprehensive and fundamentally unrestricted barrier-free design of modern information and communication technology (§ 1). It applies in particular to websites, mobile applications, electronically supported administrative processes and graphical program interfaces (§ 2). Separate provisions apply to offerings of the federal states. The regulation implements Directive (EU) 2016/2102.

For the development of criteria for apps, the use of a guideline for the evaluation of apps developed at the TU Dortmund University is helpful: examples of criteria for low barrier are usability, learnability, interface aesthetics, content, usefulness (Reh@pp-Quality 2016) . Criteria for usability are, for example, the variance of setting options: Can settings for barrier-friendliness be made individually or can assistive technologies be combined with the software (according to SGB IX §84, disabled people are entitled to barrier-free computers as aids)? Is it possible to use it exclusively on smartphones or also on other end devices? Does the respective app respond to the operating aids now integrated in most smartphones? For example, can the view of the text in the app be made larger with the help of the user interface?

Interaction designers would have to help shape this and run through various usage contexts with user testers who are dependent on the respective accessibility.

It should be considered whether a person-independent preselection should be made due to the very diverse requirements due to various sensory impairments (hearing, vision), mobility impairments, assistance technologies used, etc., or whether an app can be selected depending on the user. The latter can in turn lead to problems in everyday use if teachers have to provide the same content on different channels/apps.

Re 3: Intuitive operation is necessary for non-disadvantaged students to be additionally disadvantaged if the means of communication are difficult to learn and operate. This is conceivable, for example, if difficulties can already arise during installations, if many operating errors occur, if operating methods are awkward or not intuitively designed. A payment process that may be necessary can also play a role here.

Re 4: For use in educational institutions, a broad concept of inclusion (not only related to disabilities!) must be applied when examining the lack of barriers due to the increasingly heterogeneous prerequisites and needs of children and young people, also with regard to their backgrounds such as financial resources, level of education, family permissions and prohibitions, language skills, media skills.

The consideration of barrier-free accessibility is challenging in practice, especially because the users are very different and their needs can sometimes contradict each other: While it is necessary for visually, reading and learning disabled students that spoken voice messages can be sent, it is essential for deaf students and teachers that such are not used, but communicated in writing or through video-based sign language. However, it is ideal if the messenger provides the option for both. Sometimes there are also special versions with only text-based display of messages. Since teachers and students use different operating systems and versions, the availabilities and settings options and responses of the messenger programs would have to be tested for all variants.

5.2.2 Criteria of the accessibility test

Based on the above-mentioned principles, we developed concrete criteria according to which messenger apps/programs can be subjected to a test. The respective criteria are listed in the results table of the published study.
The selection of criteria was based on basic and essential criteria for barrier-free IT systems/apps (cf. Oliveira 2016; Reh@pp-Quality 2016; Bundesministerium für Justiz und Verbraucherschutz 2011; Aktion Mensch and Stiftung Digitale Chancen 2010). . In addition, we conducted an informal expert interview with Domingos de Oliveira, an expert in digital accessibility. From this information and the other sources, we partially developed specific test criteria for Messenger apps:

1. operability and controllability (here: basic function of writing and reading should be given)
2. Comprehensibility and learnability
3. Perceptibility (sufficient contrast for the visually impaired in the operating elements) and surface aesthetics (clear and simple design for orientation via the user interface)
4. Accessibility
5. Multimedia
6. Sustainable usability or compatibility with the operating aids integrated in smartphones

5.2.3 Summary of the accessibility test

The accessibility of messenger apps was not comprehensively tested. Although testing was our wish at the beginning of the study, it became clear during the development of the criteria as well as the first testing attempts that this was not feasible within the time and financial constraints of the project. For meaningful results, each app would have to be tested on all operating systems (iOS, Android, and various older and newer versions of each), with various assistance modes turned on (e.g., for visually impaired, mobility-impaired users, etc.). In this case, it is advisable to consult e.g. self-help associations - i.e. those directly affected. For the visually impaired, IT experts recommend WhatsApp and Threema. (Toe 2018) We have received a statement from the Bavarian Association for the Blind and Visually Impaired stating that Threema is "definitely accessible" for the visually impaired. (A. Pavkovic, pers. comm. 2021) . The messenger apps should be checked by accessibility experts. Since we did not feel able to do this, we rather tested the practicality of the apps, imagining later users who are not very tech-savvy. Therefore, we partially adopted accessibility criteria such as usability and controllability as well as interface aesthetics for testing the practicability with the aim of checking whether a switch to a new app appears promising for people who are not very tech-savvy with little learning effort.

However, we can already draw one conclusion: There is not THE one accessible messenger app - a chat client that is well suited for hearing-impaired people does not necessarily have to be equally suitable for learning-disabled people.

Recommendation:
For smaller educational institutions, it may therefore be advisable to select a messenger app depending on the composition and needs (in terms of vision, language and reading skills, etc.) of the learners and teachers. Overall, it could be worthwhile for the major educational institutions to jointly select an open-source app that could then be further developed and adapted according to accessibility needs without being dependent on the developments of the manufacturing companies. At the same time, this can then benefit the general public again.

5.3 Practicability

A data-secure, low-barrier app does not automatically have to lead to the intended usage success in an organization. Among other things, it is also relevant whether people experience this app as practical, whether they like the app, whether it provides familiar or additional useful features, whether it fits well into other organizational processes of the institution, and much more. Therefore, additional criteria for its practicality were developed. An app that is impractical to use or that cannot achieve the desired usage success due to limitations will not be able to establish itself in practice among the users - there is then a high risk that the learners will set up an informal WhatsApp group on their own and communicate via it. This third category of practicability in particular thus contains aspects that relate to the specific work in educational institutions and takes into account the inclusive mission of educational institutions to deal with diverse people among learners and teachers. With this focus, we also found relevant criteria that have hardly been developed and mapped in conventional test tables so far.

5.3.1 Basics

While the previous two test criteria were based more on a legal basis, this is not the case with practicability; here, the focus is on the functional scope and necessary concepts of integration into the educational institution, which depend on the context of use, among other things.

In addition, conceptual options for introducing and integrating the app into the institution or organization must also be clarified. These are partly dependent on the characteristics of the app (e.g., minimum system requirements, age rating). In some cases, however, they also need to be clarified independently of the characteristics of a specific app, for example, with regard to the question of whether and how it is worthwhile to generate added value at all by introducing an alternative to WhatsApp messenger if the added value of the app already being distributed is not given. To this end, concepts for the introduction, use and, if necessary, further training as well as didactic concepts for use in communication and teaching contexts should be planned. In particular, technical and organizational advantages (but also cost advantages) can also be pointed out here, which then represent actual added value.

5.3.2 Criteria of the test

Range of functions and features with characteristics of individual messengers:

1. User characteristics/age:
   How can I find out the permitted age for using an app? In the app stores, for example, the age rating for WhatsApp is given as "USK 0 years". However, the Independent Self-Regulation Body (USK) of the media industry is not legally binding here, but the General Terms and Conditions (GTC) are. These are based on the GDPR. The age rating for WhatsApp and all other messengers that collect personal data is 16 years in Germany. Personal data includes, for example, a telephone number or email address to be entered for registration. Of those messengers that were indicated above as compliant with the GDPR, SID and Wire require

the e-mail address to be provided. Thus, of proprietary systems, only Threema can be used by children younger than 16 without a declaration of consent from their legal guardians.

2. Financing:
   Can a messenger be used for free or for a fee? An app like Threema, which can be classified as secure and fulfills many features, is subject to a fee. It costs a one-time fee of 3.99 euros. Although this is only about as much as a cappuccino, the payment process itself is a major hurdle for many recipients if they do not have a credit card, do not want to disclose any of their data, or have only limited user skills. However, licenses can be purchased by the organization and given away to future users. In the case of provider-independent messengers, most apps/programs are free of charge - however, there is also the option of individual "branding" and own server operation, which is of course not possible free of charge.
3. Internal and external use:
   Does the messenger allow communication only within the institution context or can it also be used by the users for private contacts?
4. Features:
   Are popular features like calls, video chat, group chat (all encrypted) offered? Are there restrictions on sending videos, pictures, voice messages? This can also influence acceptance and everyday integration.
5. Technical effort of support and use:
   Here, it must be checked whether the use appears to be technically inexpensive for
   the later users (financing; contract hosting) and whether the operation requires technical maintenance and thus personnel, as would be the case, for
   example, with an organization's own server operation (e.g., with Mattermost or XMPP server) and whether this would be more cost-effective than licensing solutions.

6. Server: Own server operation possible?
7. Operating systems:
   Compatibility with all common operating systems, including older versions is necessary if users are to use their own devices that cannot be regulated.
8. Desktop version:
   Is a smartphone necessary for use or can the software also be used to communicate via computer and without a SIM card? This has the advantage that addressees can use computers that can be made available in the facility and that a cell phone purchase is not necessary to participate in communication if, for example, parents/guardians do not allow cell phones. The use of desktops and printers can also make documentation easier for professionals.
9. Integration into existing software usage:
   Is the Messenger app compatible with other software-supported communication and organizational processes and can it be integrated without permanent additional effort?

The following aspects and criteria do not allow the specification of characteristic values for individual apps. Rather, they are criteria to be considered when deciding whether and how, and under what conditions, a messenger deployment can be planned in the educational institution in a promising manner. Here, procedures and relevancies must be prioritized and concepts for the potential integration of Messenger into the organizational structure of the educational institution must be planned in accordance with school laws:

10. How can users be motivated to integrate the software into their everyday practice, especially if they may have already developed an everyday practice for communicating with another messenger (often WhatsApp) and there is explicit or habitual resistance to adoption?

11. Consent forms:
    Do users have to give their consent to the manufacturers or to the organization? What happens if they do not wish to do so?
12. Device ownership, service devices:
    Which devices can be used? Can/must private devices be used or can/should devices be provided by the facility?
13. Further training needs, processes:
    Are there further training needs for specialists or addressees? Is the software self-explanatory? Does its use change workflows or communication, documentation or organizational strategies that need to be clarified? Are chat addresses organization-related (function-, task- and person-related) possible?

5.3.3 Results of the test for practicability

The characteristics of the GDPR-compliant messengers were researched and recorded in the results table. Whether and how these characteristic values are significant cannot be evaluated positively or negatively; rather, it depends on the context of use and the concept in the educational institution. The development of the criteria served thus less the examination, but more as source of information of the visualization of the differences of the messengers, so that conceptional decisions become at all possible due to the characteristics. The test criteria thus fulfill their purpose particularly in their own application. This is especially true for the test of practicability - this showed what can be emphasized when introducing a messenger in educational institutions. In most cases, it is not possible to see in advance on the manufacturer's pages whether and when, for example, data must be entered during installation or what the minimum age is. In the context of vocational training for adults, a minimum age of 16 is less relevant than in an educational context where children and young people under 16 are expected.

This process of trying out the various messengers in the study team revealed how important individual features and procedures of an app can be, which are not always transparently stated on the manufacturer's website or in conventional comparison tables. The findings of the trial and error process led in part to the iterative development of an additional test criterion of practicality, which was then researched again for the apps already tested.

6 Results III: Potential of free provider-independent messengers with on-demand or self-hosted chat servers.

In addition to the provider-dependent (proprietary) messenger apps of groups A and C from individual manufacturers, there are also free messenger systems based on the international standard "XMPP" or on the matrix protocol (group B).

In the course of developing criteria for data protection, accessibility and practicality requirements of messengers in educational institutions, the potential practical advantages of free messenger systems became clear. These can only be examined in a few aspects within the scope of this study, as data protection in particular depends on the server provider. However, therein lies their potential, which will be briefly described here with the aim of classifying them (for a good overview and introduction as well as references to further sources, see Initiative Freie Messenger o.J.a; Werz 2019). .:

These include:

- several separate chat accounts (professional, private, club, other, ...) are possible;
- they can be used both with and without SIM card;
- multiple terminals can be used synchronously;
- depending on the server, the creation of a chat account is possible without personal data and therefore also for children;
- as with email, there are text-based chat apps that provide accessibility for the visually impaired because they are optimal for screen readers.

What is the main difference between provider-independent, free messengers and the well-known provider-dependent ones?

WhatsApp users can only communicate with WhatsApp users, and Threema users can only communicate with Threema users. Provider-independent messengers are open and users can communicate from all appropriately federated servers regardless of their preferred messenger app.

While opting for a provider-dependent messenger app dictates to all those involved in the educational institution which app they must use, opting for a free messenger system based on either the XMPP protocol or the Matrix protocol leaves users with choices in many respects. It even makes it possible for a communications server to be self-hosted (for example, via a state server for schools or a server run by a federal charity association) rather than commissioned, so that the data does not end up with a third party offering it. Data backups are also easy to make with contract/self-hosting (similar to email). It can be compared with communication via e-mail:

All email users, as we know, can exchange emails with all other email users, even though all users use different providers and different software. Regardless of which email address is used (whether an email address comes from the employer, from the school, from GMX, from Gmail or from a privacy-conscious provider like Posteo) and regardless of which software someone uses to write and save (e.g. the GMX software or the free Thunderbird client or the proprietary Outlook client on the desktop or the secure free K9 mail program for the Android phone): All can write messages to each other. Those who value security and encryption also install encryption software such as PGP-Open for their e-mail program.

Provider-independent chatting works according to this pattern: Everyone chooses their preferred server, from which they receive a chat address, and chooses their preferred messenger app (which is independent of the server). For example, someone who values a specific feature chooses a different messenger client

(app/program) than someone who needs better accessibility for their own needs or someone who wants to reveal their phone number (as part of the chat address). [2]
An educational institution, a school association or even an overarching state server provide the server infrastructure for this purpose, on which everyone communicates without access from third parties. Nevertheless, communication is also possible with external contacts using other servers: Unlike the proprietary Pro versions such as school.cloud etc., which have to be purchased by an institution, these messengers can then also be used additionally for private communication with family and acquaintances. As a rule, these messenger apps also allow the creation of multiple chat accounts in one app, e.g. to separate school-related and private matters.
Both the server software (Initiative Freie Messenger 2020a) as well as the messenger apps (e.g., Monal for iOS, Conversations for Android, Gajim for Windows, for a comprehensive overview of the softwares see Initiative Freie Messenger o.J.b). are free of charge and mostly open source, so that adaptations are possible, for example, for even more accessibility or individualizations.[3] These can be implemented as a development contract or possibly with own resources. Public money (from schools) thus flows into the creation of public code.
The results of our own tests can be found in the published results table in the practicality tab. With the latest findings, we would now additionally recommend testing "Siskin IM" and "Monal" for iOS devices.

In summary, the following potential benefits can be highlighted:

[2] For reasons of practicability, it might be advisable for an educational institution requiring support to recommend one messenger app for each of the major operating systems so that professional and peer support can remain manageable.

[3] For installation instructions see (Grupp 2018).

Technical:

- Separate (and multiple) chat accounts are possible;
- Simultaneous use of mobile devices and desktop/laptops with message synchronization across multiple endpoints;
- Chat with or without a smartphone;
- Chat clients for Windows/Linux/Mac and Android/iOS;
- no personal system identification number;
- not only closed chat groups, but also public chat rooms are possible;
- completely open source program code of clients and server software, which can be tested, customized and freely developed.

Organizational:

- "IT follows organization"; individual designation of chat accounts possible;
- Individualization ("branding") possible;
- in the case of self-operated chat servers, the data can be included in a backup concept;
- Connection to user management systems (e.g. LDAP) is possible;
- with vendor-independent systems, there is no need to purchase, distribute, and manage licenses because there are free apps to download at will (but chat accounts must be assigned);
- Contract data agreements can be concluded.

Cost:

- Royalty-free software is available as open source for both users and the server side.
- Funds can be awarded individually for programming assignments to improve the code.
- Server operating costs are incurred.

But free systems also have disadvantages:

- The different clients for different operating systems (like different text programs, browsers, e-mail programs, etc.) do not have a uniform user interface. Each user can/must choose their own app.
- Development is driven by many different people with different interests.
- There is no centralized, coordinated financial management.
- So far, too few development contracts have been awarded, so that the projects are less financially strong.
- The range of functions is different for each client.

The functionality as well as the usability on Android, Windows and Linux is bigger/better than on iOS.

7 Selection decisions for the messenger services "Wire" and "Threema Work" for vocational education in the project IDiT

The IDiT project went through two practical phases in which the concepts developed for teaching media competence to rehabilitation students, for the use of messengers in vocational training and for working in inclusive tandems were tested at BFW Cologne. Two different messenger services were to be used in the two phases in order to be able to generate experience and knowledge about two different apps. This chapter describes the decision-making principles and selection processes used in the two practical trial phases of the project to use the messenger services Wire and Threema Work.

7.1 Inclusion criterion: individual usability

As shown above (3.3), a distinction can be made between messenger services that can be used individually (groups A and B) and those in group C that must be provided by an institution/organization in the form of licenses (here: "institution-internal").

These intra-institutional messenger systems (Group C) can offer advantages over provider-dependent individual messengers (Group A): for example, through their fast and efficient distribution of licenses to learners, through centralized management of groups by teachers/administrators, and through the possibility of concluding a commissioned processing agreement between the educational institution and the messenger service, which ensures that the obligation to protect personal data that the educational institution has towards its employees and learners is also upheld by third-party processors, such as a messenger service.

Initially, the IDiT project did not take a closer look at internal messenger services or shortlist them for practical use. On the contrary, the first inclusion criterion was the individual (and not organization-dependent) usability of the messenger services examined. The second inclusion criterion was compliance with the GDPR without extended consents. Therefore, the provider-independent messengers (group B) were not tracked, as no own hosting was possible.

The reasons for this lie in the basic concept of the use of messengers in the project: The research interest was primarily focused on the question of how messenger services can be used as an informal supplement and voluntary additional offer in vocational training, not on their use as a formally obligatory part of training. Furthermore, it was less about testing the suitability of existing messenger services for educational contexts and more about the holistic promotion of learners' media and messenger skills (subarea: communication, data protection). More specifically, the aim was to address the everyday use of messengers - mostly WhatsApp - and to identify alternative, data-protecting messenger services that learners could use to network with each other and with their instructors, but also privately, including with people outside their educational institution.

At the same time, education and the presentation of alternatives should stimulate thought processes regarding the use of messenger apps and enable informed decisions regarding the selection of apps for private use as well. Accordingly, the introduction of a messenger in the concept for messenger services as a communication and mediation tool in vocational education and training (Murmann and Zorn 2021) and its practical testing at Berufsförderungswerk Köln is accompanied by information on the data protection aspects of messenger services in general and the risks of WhatsApp in particular.

7.2 Inclusion criterion: data protection

An absolute prerequisite for the use of a messenger in the IDiT project was the protection of personal data of the participants (especially since they participated with their private smartphones). Since the conclusion of an order processing agreement between the educational institution and the messenger service is only partially possible for individually usable messengers, the second criterion for the selection of messengers for practical testing was the GDPR compliance of the programs and services. An associated inclusion criterion was the location of the company's headquarters and the location of the servers in the EU, as the GDPR then applies regardless of additional agreements (such as the Privacy Shield, which was declared invalid by the European Court of Justice in the summer of 2020).

Accordingly, the shortlist was congruent with those messenger services that were identified as privacy-compliant based on the criteria established in the study (cf. chapter 5.1.3):

- Threema
- Hoccer (now discontinued)
- Wire
- SID (only beta version available)
- Ginlo
- Chiffry

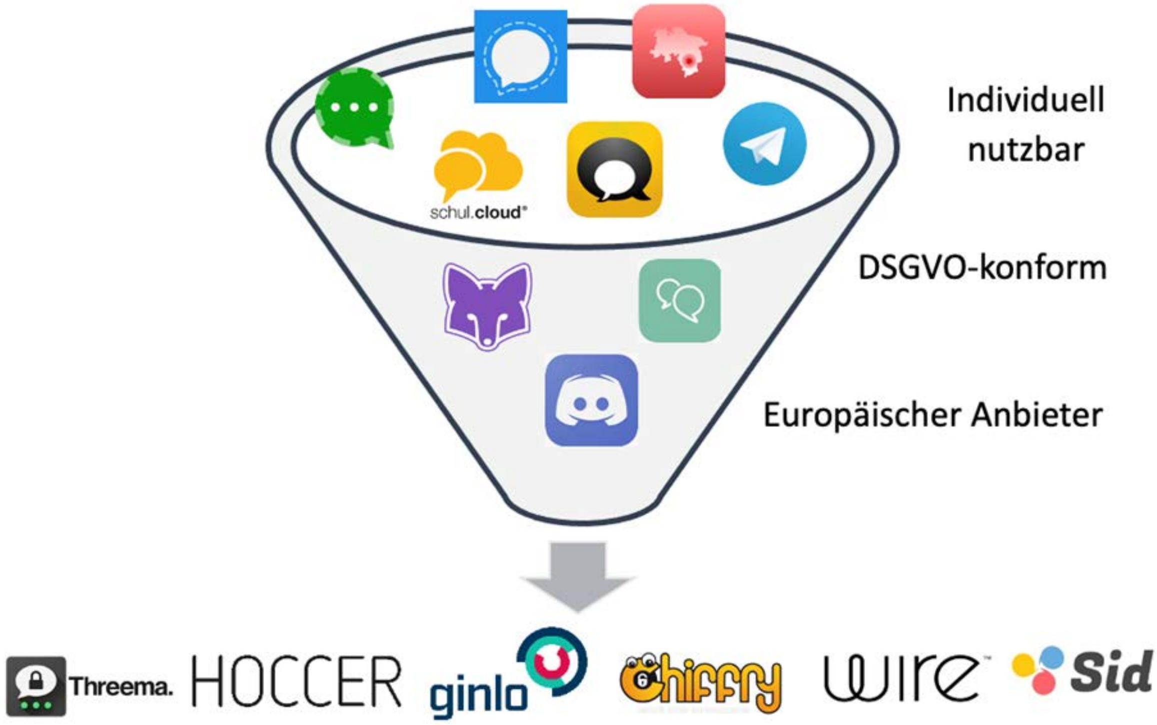


Fig. 2 Illustration of the filter criteria GDPR compliance, location/seat in EU and individual usability. These criteria were met by Threema, Hoccer, Ginlo, Chiffry, Wire and SID, as well as provider-independent messengers (but only in conjunction with a commercial server provider that enables a contract for commissioned data processing, which is why these were not considered in greater detail purely as an app).

7.3 From the shortlist to Wire and Threema (field test)

The six messenger services that made the shortlist based on the selection process outlined in 7.1 and 7.2 were tested by eight project staff over a two-month period. The observations and findings from the test phase are summarized in the "5 Practical Test in IDiT" tab of the results table (Zorn, Murmann, Harrach-Lasfaghi 2021b).

The following observations and insights regarding the shortlisted apps (Threema, Hoccer, Wire, SID, Ginlo, and Chiffry) ultimately led to the final selection of Threema and Wire:

- SID was omitted because the app was still in beta at that time, and this was also evident from the frequent occurrence of technical defects.

- Hoccer also ceased to exist due to multiple technical problems (messages were not delivered/displayed; app crash; no voice messages in certain smartphone versions). Hoccer has also been defunct since April 2020 due to insolvency.
- Ginlo: Did not run on Android 4.5. It was also temporarily discontinued during the practical phase of the project (Nov. 2019 to Feb. 2020). Is currently (as of Feb. 2021) revised and seems promising - but desktop version only in the business variant and no app for Windows smartphones.
- Threema is a technically mature app with features helpful for educational contexts (e.g., survey function, desktop application) and was selected for use in the project.
- Chiffry: Does not have the video call feature. Does not have a desktop version, so was less suitable for educational use.
- The unusual design/user interface played a role in the decision for Wire. The decision was made between the potentially more difficult access to the app on the one hand and the possibility of playful and different messenger communication on the other. It seemed appealing to offer the participants in one of the two practical sessions an app that did not correspond to the standard Messenger design.

Thus, a free Group A messenger service (Wire, IDiT Passage 1, Nov 2019 to April 2020) and a paid, institutionally procured messenger service (Threema Work, IDiT Passage 2, Nov 2020 to April 2021) (as a hybrid of Group A and C because it is institutionally procured but still allows individual use with external Threema users) were selected. Wire has an age restriction and is only approved for ages 16 and older. This did not matter for the vocational rehabilitation project context, but it may matter for younger trainees who are under 16 years old. In this case, the declaration of consent of the legal guardian is required. The age restriction results from the collection of the e-mail address; here, it should also be considered with over 16-yearolds to rather use the Pro version in order to be able to conclude an order processing agreement for the protection of the metadata as well.

7.4 From Threema to Threema Work

In IDiT Passage 2, Threema Work (organization-dependent) was ultimately used instead of Threema (individually usable). The decisive factor for this decision, which initially contradicted the considerations outlined above (7.1), was the fact that Threema Work as an app is compatible with the regular Threema app, which is also available for private individuals. This means that users of a Threema Work license can easily communicate with users of a Threema license. Contacts from the regular Threema app are marked as private in Threema Work (icon: house); contacts from Threema Work are marked as professional in the regular version (icon: briefcase). [4] Thus, the central reason why organization-dependent services should not be used in the project does not apply to Threema Work. However, the advantages that Threema Work has over the regular Threema app are exactly those that other organization-dependent messengers also have. For IDiT, the quick and easy distribution of licenses to participants played a particularly important role. The costs for the licenses were borne by the project, and under these circumstances the use of Threema Work was the most efficient solution for all parties involved (participants, trainers, project staff) - while at the same time meeting the requirement that the app should also be usable privately.

Overview: Advantages of Threema Work over Threema

- User management via central administration: The Management Cockpit provides an overview of active users, their IDs and the licenses used.
    - Access data management

[4] What remained unclear was: How does this behave when there are multiple employers (which can actually happen)? Is there a separation of the respective contacts?

  - Disconnect Threema IDs
  - Delete Threema IDs
- Individualization
  - In-app logo
  - internal contact list
  - User support via in-app form
- App configuration
  - Configure the app for users directly in the management cockpit. With Threema MDM, all or specific user app settings can be customized and specific features can be disabled.
  - Statistics: anonymized data analysis
  - License management
  - Manage access permissions: Appoint additional administrators and users for the Management Cockpit and set permissions.

7.5 Summary: Selection decisions of a messenger for vocational training in the IDiT project.

In summary, it should be noted: The decisive inclusion criteria for the selection of messengers used in the practical phase of the IDiT project at the Berufsförderungswerk Köln were the GDPR conformity of the programs as well as the domicile of the offering companies and the location of the data processing servers in the EU. For conceptual reasons - the guiding idea was more the promotion of general media competence of the participants, less the testing of existing offers of messenger services for educational contexts - importance was attached to the fact that a messenger should also be usable privately and for communication with people who do not belong to one's own educational institution. Therefore, organization-dependent messenger services were initially excluded.

The final selection of Wire and Threema was based on the findings of a practical test conducted within the project, which focused in particular on the features, practicality, and design of the messengers. In favor of the richness of variants within the research project, Wire was selected precisely because of its rather atypical interface aesthetics, despite initial concerns about possible access difficulties. Since Threema offers Threema Work, which on the one hand offers the advantages of organization-agnostic messenger services, but on the other hand remains compatible with the regular Threema app and thus can be used privately without any problems, the decision was ultimately made in favor of Threema Work, contrary to the original assumption to exclude organization-agnostic messengers.

How both messengers prove themselves in practical use and where open questions arise as well as challenges and opportunities become visible is to be evaluated.

8 Summary

The article described the requirements for messenger communication in educational institutions and explored the question of which criteria were used as a basis for decisions on messenger communication in the Diakonie Michaelshoven Vocational Training Center in the IDiT project. To this end, the article systematically presented requirements for the use of messengers in educational institutions that differ from the requirements of private individuals and developed three areas with criteria that need to be examined when deciding on a messenger offering: data protection, low barriers, and practicability for the intended use.

Shortcomings in the applicability of GDPR mean that popular messengers are not suitable for use in schools or social work [5]. A major problem with data protection is the lack of protection of address entries on a device as well as the handling of metadata. However, data protection alone is not a sufficient criterion. The more data-secure providers can be tested according to developed test criteria of practicability

[5] E.g. WhatsApp, Telegram, Viber, Skype, Signal

and barrier-friendliness. Here, initial research and tests show that DSGVO compliance (e.g., Threema, Wire, Hoccer, XMPP-based apps) is already accompanied by reductions in practicability and low barriers.

However, interesting alternatives exist among those messengers which are offered by the institution by means of contracts [6]and for which agreements on commissioned processing can be made with the manufacturers in the contract. Without agreements on data processing with the manufacturers/server operators, the use of free messengers by institutions is (at least) in a gray area, even if they comply with the GDPR, when it comes to confidentiality obligations or social data exchange. It must be clarified how this is to be legally evaluated in the case of end-to-end encryption if, for technical reasons, only the two communication partners have access to the communication and no metadata is stored by the provider.

In addition to paid offers for contract/remote hosting of both organizational solutions and free messenger systems, there is also the possibility of own server operation for processing the data with e.g. Mattermost (open source team solution) or normal (also open source) chat servers based on XMPP[7] .

An Excel overview of detailed messenger searches according to the requirements and criteria shown was created as part of the BMBF-funded IDiT project (Zorn, Murmann and Harrach-Lasfaghi 2021b).

The further development of criteria for organizational feasibility or practicability should therefore not take place exclusively with technical, but also with pedagogical professionals in pedagogical contexts and should be examined before organizational decisions are made, because technology decisions influence pedagogical action

[6] Examples of this are organizational solutions such as Threema Work/Education, WeChat, Wire Pro/Enterprise, SchulCloud or others - but also provider-independent messengers). For reasons of practicability and acceptance, it could be worthwhile to ensure that not only internal organizational communication is possible, but also private communication - if desired by users.

[7] https://www.freie-messenger.de/sys_xmpp/server/ ; Instruction: https://www.freie-messenger.de/dateien/conversations/Anleitung_Conversations.PDF

(Kutscher et al. 2020) . Because the decisions to be made must be examined comprehensively and have an impact on work processes, a decision by upper hierarchical levels is advisable, since this cannot be expected of individual specialists.

Presumably, further technical development of privacy-protecting software is necessary for the context in question, so that it can increasingly also fulfill the criteria described in the points on barrier-friendliness and practicability. Cooperation at the federal, state or association level and with staff units of the state data protection commissioners should be considered because of the complexity involved. It should also be considered whether promising open-source products that are easy to host (possibly with the XMPP protocol) could be used to provide reliable, free software alternatives by the states or through cooperation between the charitable associations.

Professionals and addressees would thus be supported in their communication needs. Moreover, non-action on the part of the institutions does not fundamentally prevent the use of messengers. Rather, it is to be feared that this will increase the informal use and spread of those messengers that do not protect data, do not respect privacy, do not respect accessibility, and that this will increasingly lead to exclusions when, for example, learners communicate with each other via WhatsApp in resignation for lack of alternatives despite growing awareness of data protection issues. In this respect, educational institutions are also called upon to find and offer solutions here in accordance with their educational mission. By demonstrating the feasibility of data-protecting messenger communication, they could promote the media literacy of a broad section of the population in the dimensions of media knowledge, media use, media criticism and media design (Baacke 1996) of a broad section of the population.

A research desideratum for the evaluation of such field research becomes clear. Further research can provide insights into how learners communicate with WhatsApp alternatives and what other aspects and criteria should thus inspire decisions and concept developments for Messenger use in educational institutions.

II Bibliography

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.

III Appendix: Messenger provider websites

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/
School.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/

Various 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/