Gunnar von Spreckelsen

Gutachten über die Nutzung von Anwendungen für die interne Kommunikation im Verein Tura-Hechthausen

Version 2 (03. Februar 2021)

Inhalt

1.) Vorwort

Im Verein Tura-Hechthausen führen Verantwortliche Video-Telefonien durch, Vereinsmitglieder bilden Chat-Gruppen innerhalb ihrer Messenger-App, um sich mit Daten auszutauschen. Einige Sparten-Verantwortliche erstellen Live-Videos zur Präsentation über youtube.

Im Folgenden wird dargestellt, wie die gesetzlichen Bestimmungen und andere Datenschutz-Anforderungen durch die relevanten Anwendungen erfüllt werden. Anschließend erfolgt eine Selektierung von passenden Tools zur Video-Telefonie und Messaging. Tura-Hechthausen gewährleistet durch die Vorgaben der Tools für die vereinsinterne Kommunikation einen Schutz seiner Mitglieder im Rahmen der Rechtssicherheit.

2.) Definition der Anforderung

Die Video-Telefonie- und Messenger-Anwendung sind im Rahmen der Einhaltung der Datenschutz-Gesetze hinsichtlich der Speicherung und Behandlung von Daten wie Telefonnummern und dem eigentlichen Umgang und Nutzung von Medien-Daten von

Bildern oder Videos zu bewerten. Durch ein begrenztes Budget sind auch die Betreiber-Kosten der Apps relevant.

3.) Darlegung der relevanten Bestimmungen durch die Datenschutzgesetze

Neben der Europäischen Datenschutzgrundverordnung (EU-DSGVO) gilt das nationale neue Bundesdatenschutzgesetz (BDSG-neu). Die DSGVO enthält zahlreiche Öffnungsklauseln, damit ist gemeint, dass „an diesen Stellen die Regelungen offengehalten werden, damit sie auf nationaler Ebene konkretisiert werden können. Diese Aufgabe übernimmt das BDSG-neu“ [1].

Nach der EU-DSGVO kann der Daten-Übermittler bzw. Nutzer jederzeit über seine Daten verfügen und der Anbieter hat entsprechende Maßnahmen umzusetzen, um den entsprechenden Schutz zu gewährleisten. Nach Art. 5 DSGVO dürfen Daten „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden“ [2]. Da es in der EU-DSGVO keine weiteren spezifischen Einschränkungen für die Anforderungen an Messenger- oder Telefonie-Apps gibt, erfüllen viele Systeme demnach alle Anforderungen.

Auch das BDSG-neu erklärt keine spezifischen Anforderungen an die Betreiber von Messenger-Apps, kein Paragraph berücksichtigt spezielle Anwendungsfälle für Messenger-Szenarien, siehe das BDSG-neu [3]. Es regelt im Grunde das Widerrufs-Recht und das Recht auf Einsicht und Löschung, diese beiden Kriterien sind auch maßgeblich für die praktische Bewertung von Datenschutz-Maßnahmen. Für eine charakteristischere weitere Einordnung stellt der Beauftragte für den Datenschutz der EKD (BfD EKD) folgende Kriterien dar:

1. Ende-zu-Ende-Verschlüsselung der über den Messenger-Dienst ausgetauschten personenbezogenen Daten muss gewährleistet sein.
2. Der Anbieter nutzt die empfangenen personenbezogenen Daten ausschließlich für Zwecke der Übertragung von Nachrichteninhalten zwischen den Teilnehmenden einer Unterhaltung.
3. Unberechtigte Weitergabe von Kontaktdaten an den Messenger-Anbieter – insbesondere durch Übermittlung des auf dem eingesetzten Endgerät gespeicherten Telefonbuchs – muss ausgeschlossen sein.
4. Datenschutzniveau im Land des Messenger Anbieters bzw. am Verarbeitungsort muss dem der DS-GVO oder des DSG-EKD entsprechen

Das letzte Kriterium wird in der Stellungnahme ergänzend genannt und kann durch Angemessenheitsbeschlüsse (Teilnahme am EU-US-Privacy Shield Abkommen) erreicht werden [4]. Die Vereinbarung für den Datenaustausch zwischen Europa und den USA (EU-US-Privacy Shield Abkommen) ist aktueller aber vom höchsten EU-Gericht gekippt worden [5].

RA Michael Röcken [6] stellt es als Frage-Checkliste dar:

- Hat der Anbieter seinen Sitz in der EU?
- Stehen die Server des Anbieters in der EU?
- Stellt der Anbieter eine Datenschutzerklärung zur Verfügung?
- Stellt das Angebot eine Ende-zu-Ende-Verschlüsselung der Kommunikation sicher?
- Welche Informationen dazu stehen zur Verfügung?
- Stellt der Anbieter Informationen darüber zur Verfügung, welche Daten an andere Stellen weitergegeben werden, in welchen Länder die einzelnen Komponenten seiner Infrastruktur lokalisiert sind und zur Sicherheit der Infrastruktur?

Ein Anwalt mit dem Schwerpunkt Medien-Recht würde auch WhatsApp als Messenger nicht ausschließen. Wer Daten innerhalb einer Gruppe empfängt, hat vorher sein Einverständnis durch den Beitritt in diese Gruppe erteilt. Umgekehrt entzieht dieser Nutzer sein Einverständnis durch den Austritt. Bei der Videotelefonie mit Skype im Rahmen von gespeicherten Daten in den USA wird angemerkt, dass dieses eher ein Problem von Microsoft ist, als Benutzer muss der Initiator die Teilnehmer darauf hinweisen, dass deren Daten in anderen Ländern als Deutschland gespeichert werden können, ohne den Datenschutz-Regelungen der EU oder Deutschlands zu entsprechen. Wenn Videos in Echtzeit als Stream zum Beispiel über youtube präsentiert werden, muss anderen Personen, die ebenfalls Bestandteil dieser Videodaten sind, deren Recht auf Widerruf mitgeteilt werden. Jugendliche unter 16 Jahren sollten sich bei der Verbreitung von vereinsinternen Daten das Einverständnis der Eltern geben lassen.

4.) Auswahl des Messengers

In die aktuelle Auswahl fallen die Instant-Messenger Threema, WhatsApp, Signal, Wickr, Telegram und Wire.

Wire war vor 2 Jahren eine ausgezeichnete Lösung, leider traten auf mehreren Handy-Installationen zu häufig Bugs auf und die App hat sich im Laufe der Zeit zu einem „Teamarbeit-Tool“ mit zu hohen monatlichen Gebühren entwickelt. Mitarbeiter der Bundesregierung testen aktuell Wire.

Die Verwendung von **WhatsApp** als kommerzielle Variante mit der Nutzung von Daten durch Facebook und Hosting in den USA kann keine Variante darstellen, auch wenn entsprechende mediale Darstellungen von Facebook gegenteiliges behaupten. Letztendlich werden die Benutzer-Daten immer vermarket und Facebook gewährt

keinen Einblick in die gespeicherten Daten. Damit befassen sich diverse Rechtskanzleien wie z.B. Rechtsanwalt David Oberbeck [7], wobei noch zwischen dem Einsatz von WhatsApp in Unternehmen, von natürlichen Personen oder innerhalb eines Vereins unterschieden werden muss. Auch wenn ein Medien-Rechtler wie bereits kurz beschrieben WhatsApp rechtlich nicht verbieten würde, sollte Tura dennoch darauf verzichten. Zum Teil werden datensensible Dokumente versendet oder Medien-Daten, auf denen Kinder oder Jugendliche verzeichnet sind.

Telegram wird zum Beispiel von Personen genutzt, die Protest-Aktionen wie im Iran organisieren und dafür ein Höchstmaß an Anonymität erhalten wollen. Die App wird auch als Messenger des Dark Webs bezeichnet. Für TURA ist sie keine Alternative, da sie zu undurchsichtig ist und möglicherweise von dubiosen Personen gegründet wurde, „hinter dem Messenger-Dienst stecken die russischen Brüder Nikolai und Pawel Durov“ [8]. Ein Kritik-Punkt ist auch das eigenentwickelte Protokoll *MTProto,* auf dem Telegram basiert, weil Experten die Sicherheit durch Vermischung teilweise veralteter Verschlüsselungs-Algorithmen anmerken [9]. Telegram verwendet standardmäßig keine Ende-zu-Ende-Verschlüsselung und speichert die gesamte Nutzer-Kommunikation auf Servern.

Wickr ist ähnlich wie Threema.Work ein Tool für die Kommunikation im Team. Ein Administrator verwaltet Benutzer- und andere Ressourcen, für 6 Euro im Monat können eine beliebige Anzahl an Benutzern bis zu einem GB Daten verbrauchen, das Ausschlusskriterium ist auch das Hosting in den USA. Es stellt sich die Frage, ob die Vereinsführung den Mitgliedern nicht ein Teamarbeits-Tool aufzwingt, dass lediglich für die Vereinskommunikation genutzt werden kann. Die Vereinsmitglieder würden vielleicht lieber ein Tool bevorzugen, dass sie sowohl privat als auch im Vereins-Umfeld nutzen würden. Da Wickr und auch Threema.Work anderseits Profitools mit garantierter Anonymität sind, kann man innerhalb des Vereines darüber diskutieren. Threema Work „ist mit der Europäischen Datenschutz-Grundverordnung (DSGVO) konform. Als Schweizer Unternehmen ist Threema zusätzlich dem strengen Schweizer Datenschutzgesetz (DSG) sowie der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) unterworfen [10]. Leider ist der Preis mit 1.40 Euro je Gerät und Monat nicht realisierbar.

Um eine Differenzierung zwischen Threema oder Signal vorzunehmen, ist eine umfangreichere Stellungnahme notwendig: Zunächst können bei Threema Dateien je maximaler Größe bis zu 50 MB versendet werden. Bei einer älteren Version wurden immer wiederkehrende Probleme mit der Videotelefonie festgestellt, Threema wirbt allerdings mit der aktuelleren Version mit einer verbesserten Stabilität von Video-Anrufen.

Tabelle 1: Vergleich zwischen Threema und Signal nach [11], Thema Sicherheit

Kriterium	Beschreibung	Threema	Signal

Ende-zu-Ende-Verschlüsselung	Die übertragenen Daten über alle Übertragungsstationen hinweg können nur die Kommunikations-Partner (die jeweiligen Endpunkte der Kommunikation) entschlüsseln.	Ja, uneingeschränkt	Ja, uneingeschränkt
Quellcode veröffentlicht	Als Qualitätsmerkmal der Anwendung dient die öffentliche Veröffentlichung des Codes, dadurch erhöht sich die Qualität der Sicherheit durch Prüfungen auf Schwachstellen von anderen Experten	Ja, uneingeschränkt	Ja, uneingeschränkt
Nutzung Telefonnummer	Besteht durch den Nutzer die Notwendigkeit zur Eingabe seiner Telefonnummer, die dann ebenfalls auf dem Anbieter-Server gespeichert wird?	Der Dienst kann ohne die Verwendung einer Telefonnummer verwendet werden. Hier wird bei der Einrichtung eine Threema-ID generiert, die keine Rückschlüsse auf Personen zulässt.	Signal lässt sich nicht ohne Telefonnummer verwenden. Allerdings existieren weitere Mechanismen, die einen erweiterten Schutz zur Verfügung stellen. Der Empfänger kann eine neue Anfrage anonym ablehnen, so dass der Absender nicht erkennt, ob die Anfrage erfolgreich übermittelt wurde.
Datenschutz-Richtlinien	Die Daten sollten nach Möglichkeit auf deutschen Servern gehostet werden und das BDSG-neu erfüllen	Konform mit: Europäischer Datenschutz-Grundverordnung, Schweizer Datenschutz-Gesetz und	Signal betreibt die Server in den USA. Im Zweifelsfall muss das Unternehmen US-Behörden Zugriff auf Daten

		Verordnung zum Bundesgesetz über den Datenschutz	gewähren. Aufgrund der Verschlüsselung hat Signal zwar keinen Zugriff auf Nachrichteninhalte, personen-bezogene Daten wie die Telefonnummer könnten jedoch weitergegeben werden.

Tabelle 2: Vergleich zwischen Threema und Signal nach [11], Thema Funktions-Umfang und Hersteller-Info

Funktionalität	Vergleich
allgemein	Bedienung und Funktionsumfang sind bei beiden Apps ähnlich wie mit WhatsApp. Bei beiden können (Sprach-)Nachrichten, Bilder und Videos ohne Probleme versendet werden. Sprach- und Videoanrufe sind bei beiden Messengern möglich, jedoch lassen sich bei Signal im Gegensatz zu Threema Gruppenanrufe mit bis zu acht Personen tätigen.
Preis	Threema kostet je Endgerät einmalig 3.99 Euro (IOS oder Android), Signal ist als Stiftung kostenlos und finanziert sich vollständig von Spenden
Zusatz-Tools	Mit Threema-Web als Web-Client kann Threema mit dem gleichen Funktionsumfang im Browser benutzt werden. Signal stellt eigenständige Programme für Windows, Linux oder Mac zur Verfügung, dabei ist eine aktive Installation auf einem mobilen Gerät aber Voraussetzung.
Hersteller	Threema ist in als Unternehmen in Pfäffikon in der Schweiz angesiedelt, Signal befindet sich als Stiftung in Kalifornien

5.) Technische Erläuterung zur Funktionsweise

Moderne und sichere Messenger übertragen die Mediendaten (Bilder, Video und Chats) per Ende-zu-Ende-Verschlüsselung, ein vielverwendetes Übertragungs-Protokoll dafür ist das Signal-Protokoll. Da die Daten direkt über die „Eingabe in Internet“ beim Empfänger landen, wird für die Kommunikation kein Server benötigt, der irgendwelche Daten speichert. Ein eingesetzter Server speichert lediglich die darüber hinaus entstehenden Daten wie z.B. Kontakte des Nutzers, in der Regel

ebenfalls verschlüsselt. Eine direkter Videoanruf kann beispielsweise auch über den Firefox-Browser erfolgen [12]. Zukünftig wird genauer erforscht und getestet, ob der Verein nicht einen eigenen Server mit der entsprechenden Messenger-Installation aufbauen sollte, um dadurch vollständig losgelöst agieren zu können.

6.) Auswahl des Instant-Messengers

Die Kernfragen bei Signal lauten, ob der Stiftung vertraut werden kann, wirklich seriös mit den Daten umzugehen und das diese Stiftung dauerhaft erhalten bleibt. Snowden und die EU-Kommission empfehlen Signal [13], die Stiftung ruft weltweit zu Spenden auf, Amazon unterstützt Signal über das Smile-Programm mit 0.5 % der Einkaufssumme je Bestellung. Signal könnte bei Geldknappheit nach dem Wikipedia-Vorbild Spenden einsammeln. Durch die gute Sache der Anonymität und Leistungsfähigkeit wird Signal in Zukunft einen guten Ruf mit sozialem Hintergrund haben und kann deshalb auch uneingeschränkter mit immer mehr Nutzern wachsen und die benötigten Infrastrukturen finanzieren. Dadurch sind die Entwickler, die hinter Signal stehen, motiviert und finanziert und werden uns in Zukunft mit den neuen Erweiterungen versorgen.

Threema als Wirtschafts-Unternehmen passt sich mit dem Angebot der Standard-Messenger-Version den Markgegebenheiten an. Signal hat seine Nutzungszahlen innerhalb weniger Tage von 10 auf 50 Millionen verfünffacht, auch Threema hat starken Zulauf erhalten, gibt aber keine weiteren Daten bekannt [14]. Offensichtlich ist für den Benutzer der zu zahlende Preis für die Threema-App durchaus ein Argument, sich eher für Signal zu entscheiden, Signal wird das zukünftige Wikipedia der anonymen Kommunikation, die Kapazitäten für die Gruppen-Video-Telefonie von maximal derzeit 8 Personen werden stetig erhöht werden. Innerhalb der kommenden fünf Jahre soll Signal mehr als eine Milliarde Nutzer haben und zukünftig soll Signal auch ohne Telefon-Nummer-Preisgabe verwendet werden können. [15]

7.) Auswahl des Videokonferenz-Software

Auch eine Videokonferenz-Software zeichnet sich durch eine transparente Ende-zu-Ende-Verschlüsselung mit der Speicherung von Metadaten oder anderen notwendigen Daten auf deutschen Servern und der Erfüllung von Datenschutz-Gesetzen aus. TURA mit einem begrenzten Budget muss sich an einer möglichst kostengünstigen Variante orientieren. Hier ergibt sich eine Lösung, die auf die finanzielle Unterstützung durch MS beruht. Microsoft gewährt Vereinen mit einem gemeinnützigen Hintergrund 10 kostenlose 365-Business-Abos, jedes weitere Abo kostet mit 5 US-Dollar netto fast die Hälfte (aktuell kosten 5 US-Dollar 4,16 Euro) [16]. Der Konzern ist durch den Kauf von Skype zu einem führenden Anbieter von Video-

Telefonie aufgestiegen, MS Teams stellt eine gute Lösung dar. Dem Verein würde dann neben dem üblichen Office-Produkten auch die Cloud OneDrive zum Teilen und speichern von Dokumenten zur Verfügung stehen, interessanterweise ist dann eine „DSGVO-konforme und nachweislich sichere Datenspeicherung in deutschen Rechenzentren“ [17] garantiert.

Quellen-Nachweise:

[1] Geltungs-Bereich und Unterscheidung zwischen EU-DSGVO und BDSG-neu
https://www.datenschutz.org/bdsg-neu/

[2] EU-DSGVO Art. 5 DSGVO
https://dsgvo-gesetz.de/art-5-dsgvo/

[3] BDSG-neu
https://dsgvo-gesetz.de/bdsg/

[4] Datenschutzkonformer Einsatz von Messengern in kirchlichen evangelischen Stellen
https://www.ensecur.de/datenschutzkonformer-einsatz-von-messengern-in-kirchlichen-evangelischen-stellen/

[5] EuGH erklärt Privacy-Shield-Abkommen für ungültig
https://www.e-recht24.de/artikel/datenschutz/12236-eugh-erklaert-privacy-shield-fuer-ungueltig.html

[6]
RA Michael Röcken, Webinar Mitgliederversammlung und Vorstandsbeschlüsse in Corona-Zeiten

[7] Rechtsanwalt David Oberbeck: Ist WhatsApp in Unternehmen mit der DSGVO vereinbar?
https://www.datenschutzkanzlei.de/ist-whatsapp-in-unternehmen-mit-der-dsgvo-vereinbar/

[8] Telegram-Kritik: Wie gefährlich ist der Messenger-Dienst wirklich?
https://www.basicthinking.de/blog/2020/11/11/telegram-kritik-verschwoerungstheorien/

[9] Artikel zur Sicherheit der Verschlüsselung bei Telegram

https://www.golem.de/news/telegram-der-wertlose-krypto-contest-1402-104871-2.html

[10] Rechts-Sicherheit von Threema.Work
https://work.threema.ch/de/haeufige-fragen#security

[11] Vergleich Threema vs. Signal
https://praxistipps.chip.de/threema-vs-signal-messenger-apps-im-vergleich_39301

[12] Direkte Video-Telefonie über den Firefox-Browser
https://www.pc-magazin.de/ratgeber/firefox-hello-video-chat-im-browser-anleitung-3196147.html

[13] Empfehlung für Signal durch Snowden und EU-Kommission
https://www.hna.de/netzwelt/whatsapp-unsicher-edward-snowden-empfehlen-signal-zr-13563515.html

[14] Nutzung von Signal verfünfacht
https://www.golem.de/news/weg-von-whatsapp-signal-verfuenfacht-nutzer-in-kuerzester-zeit-2101-153403.html

[15] Darum ist Signal das bessere WhatsApp
https://www.stern.de/digital/smartphones/signal--darum-ist-der-dienst-besser-als-whatsapp-und-telegram-9172812.html

[16] Microsoft Nonprofit-program
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4KyRf

[17] Microsoft 365 Leistungs-Übersicht
https://www.microsoft.com/de-de/microsoft-365/business/compare-all-microsoft-365-business-products-b?market=de