Nutzenabwägung

Nutzung digitaler Medien und Videokonferenztools in der A6-Fachabteilung Gesellschaft

Verfasserin:
Kompetenzstelle Digitale Gesellschaft
A6-Fachabteilung Gesellschaft

Stand: April 2021

Das Land Steiermark

Inhaltsverzeichnis

Kommunikation

In diesem Kapitel geht es rein um die Kommunikation mit Zielgruppen über nachfolgend behandelte Messenger-Dienste, bzw. die in Sozialen Netzwerken integrierten Chatfunktionen, also um die Frage, welche Plattformen erfüllen die realitätsbezogenen, praxisnahen und datenschutzrechtlichen Voraussetzungen für Kontaktaufnahme, persönliche Gespräche, etc. Die Bekanntmachung und Darstellung der eigenen Angebote werden in einem eigenen Kapitel behandelt.

Allgemeines

Der Einsatz von Messenger-Diensten und Sozialen Netzwerken in der Kinder- und Jugendarbeit erscheint, besonders im medienpädagogischen Kontext, als durchaus sinnvoll, da damit eine Orientierung an der Lebenswelt der Kinder und Jugendlichen einhergeht. Die Kommunikation mit Kindern und Jugendlichen über Soziale Netzwerke, stellt jedoch auch nach Einführung der DSGVO[1] eine rechtlich nicht genau definierbare Grauzone dar. Grundsätzlich dürfen Jugendliche in Österreich erst ab dem 14. Lebensjahr[2] der Verarbeitung personenbezogener Daten wirksam zustimmen, davor ist eine Einwilligung der Eltern erforderlich. Laut DSGVO müssen sich sämtliche Dienste „unter Berücksichtigung der verfügbaren Technik mit angemessenen Anstrengungen“ sogar vergewissern, ob Eltern oder andere Sorgeberechtigte mit der Nutzung einverstanden sind bzw. eine Einwilligungserklärung abgegeben haben. Jugendarbeiter*innen sollten bei der Nutzung der nachfolgend beschriebenen Plattformen, möglichst vor der Kontaktaufnahme zu den Kindern und Jugendlichen, darauf hinweisen, dass unter-14-jährige die Plattform nur nutzen sollten, wenn die Eltern auch damit einverstanden sind.

Im Idealfall sollte eine Einverständniserklärung, die ohne Formzwang, also mündlich in einem persönlichen Gespräch (auch per Telefonat), besser aber schriftlich per Mail, SMS von den Erziehungsberechtigten eingeholt werden.
Sollten Jugendarbeiter*innen, Erziehungsberechtigte, oder Lehrpersonen herausfinden, dass auch unter-14-jährige Klient*innen, Kinder oder Schüler*innen Messenger-Dienste und/oder Soziale Netzwerke ohne Einverständnis nutzen, wird dies keine rechtlichen Konsequenzen für ihn/sie haben.

Die Jugendlichen verstoßen zwar gegen die Nutzungsbedingungen von WhatsApp, Instagram, TikTok und co., jedoch handelt es sich hierbei um kostenlose Dienste, aus dem Verstoß gegen die Nutzungsbedingungen heraus entsteht also keinerlei bezifferbarer Schaden für die Anbieter (eher im Gegenteil!).

Darüber hinaus kommt mangels vorhandener Geschäftsfähigkeit durch Nichterreichung des vorgeschriebenen Mindestalters gar kein gültiger Vertrag zustande. Somit sind auch etwaige vertraglich festgelegte Konsequenzen als zahn- und haltlos zu betrachten. Weiters können Jugendliche vor Vollendung des 14. Lebensjahres für Vergehen prinzipiell nicht verantwortlich gemacht werden.

---

[1] Die Datenschutzgrundverordnung trat am 25. Mai 2018 in Kraft.
[2] Art. 8 DSGVO sieht sogar das vollendete 16. Lebensjahr vor, jedoch mit dem Zusatz, dass „Mitgliedstaaten durch Rechtsvorschriften […] eine niedrigere Altersgrenze vorsehen…“ dürfen. Diese darf jedoch nicht unter dem vollendeten 13. Lebensjahr liegen.

Social Media

Rechtliche Grundlagen und relevante Funktionshinweise

WhatsApp

WhatsApp ist eine Messenger-App zum Versenden von Textnachrichten, Fotos, Videos, Dokumenten, Sprachnachrichten oder Audiodateien. Unterhaltungen können nicht nur zu zweit, sondern auch in Gruppen mit bis zu 256 Personen geführt werden.

Die WhatsApp-Gruppe ist mittlerweile ein wichtiges Instrument für die Organisation und den Austausch in der Familie, als Kommunikationsplattform rund um den schulischen- oder Arbeitsalltag, bzw. im Freundeskreis.

Seit 2015 besitzt WhatsApp auch die Funktion der Videotelefonie, was sich besonders bei Reisen oder sonstigen Auslandsaufenthalten als sehr praktische und kostengünstige (sofern über WLAN) Alternative zu gewöhnlichen Telefonaten erweist.

WhatsApp ist das beliebteste und wichtigste Kommunikationstool der Jugendlichen in Österreich. 91% der 11- bis- 17-Jährigen sind über diese Plattform erreichbar[3] und machen den Messenger-Dienst damit zu einem unerlässlichen Kommunikations-Tool in der Arbeit mit jungen Menschen.

Rechtliche Grundlagen

- **WhatsApp Nutzungsbedingungen**: Nutzung ab dem 16. Lebensjahr (bzw. "...das in deinem Land für die Registrierung bzw. Nutzung unserer Dienste erforderliche Alter") erlaubt
- **DSGVO Österreich[4]**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze

Welche Daten werden gesammelt?

- Alle Daten, die der Nutzer angibt und nicht durch die **Ende-zu-Ende-Verschlüsselung[5]** geschützt sind.
- Ständiger Zugriff auf das komplette Adressbuch
- Weitergabe sämtlicher Kontaktdaten schon bei der Installation sowie nach Aktualisierungen
- Übermittlung von Metadaten (Handymodell, Betriebssystem, WLAN, Standort)
- Übermittlung öffentlicher Daten wie Profilbild, Status, Info und "Zuletzt Online".

[3] Siehe Jugend-Internet-Monitor 2020: https://www.saferinternet.at/services/jugend-internet-monitor/
[4] Das empfohlene Alter laut DSGVO ist nicht vergleichbar mit Altersbeschränkungen auf digitalen Spielen (USK, PEGI) oder Filmen (FSK), sagt also weder etwas über eventuelle Gefahren aus, noch stellt es eine Warnung vor nicht altersgerechten Inhalten dar. Es geht einzig und allein um die Frage, ab wann Jugendliche die nötige Reife besitzen, um eigenständig eine Einwilligung zur Datenverarbeitung erteilen zu dürfen.
[5] Daten werden über alle Übertragungsstationen hinweg bis zum Empfänger verschlüsselt. Weder der Anbieter des Messenger-Dienstes (in dem Fall Facebook, zu dem WhatsApp seit 2014 gehört), Telekommunikationsanbieter oder Internet-Provider können auf die Inhalte der Nachrichten zugreifen.

Die Verwendung von WhatsApp (besonders für berufliche Zwecke) ist grundsätzlich nicht datenschutzkonform

Mögliche Ausnahmen[1]:

- **Ausnahme 1: Art. 6, Abs. 1, lit. f DSGVO: "Datenverarbeitung zur Wahrung berechtigter Interessen"**
  - Vorhandensein eines rechtlichen, tatsächlichen, wirtschaftlichen oder ideellen Interesses.
  - Datenverarbeitung muss erforderlich sein, um das Ziel bzw. den Zweck der Verarbeitung zu erreichen.
  - Grundrechte und Grundfreiheiten der betroffenen Person müssen überwiegen[2]
  - Einwilligung zur Datenverarbeitung
  - Transparenz (die betroffene Person muss über Art und Umfang der Datenverarbeitung jederzeit informiert sein)
  - Hinweis auf permanentes Widerspruchsrecht der betroffenen Person
- **Ausnahme 2: Erwägungsgrund 38, DSGVO**: Datenschutzrechtliche Interessen nach DSGVO dürfen **Kinder und Jugendliche** nicht davon abhalten, Präventions- oder Beratungsdienste in Anspruch zu nehmen.

[1] Hierbei handelt es sich um Einschätzungen von Datenschutz-Juristen, es gibt dazu noch keine Präzedenzfälle

[2] Die Person, deren Daten verarbeitet werden, wird in der DSGVO als betroffene Person bezeichnet, die datenverarbeitende Person heißt Verantwortlicher.

Relevante Funktionshinweise

- **WhatsApp ist kostenlos**.
- Übertragung von Inhalten ist sehr sicher (**Ende-zu-Ende-Verschlüsselung**)
- Datentransfer bis zu einer Größe von 64MB ist möglich.
- Gruppen-Chats mit bis zu 256 Personen sind möglich, allerdings liest dabei jeder alles mit und sieht auch die Telefonnummer, bzw., nach einmaliger Interaktion in der Gruppe, auch die Info (meistens der selbstgewählte Name auf WhatsApp)
- Möglichkeit eines Broadcast: Gruppe wird gebildet, Nachricht kann an mehrere Teilnehmer*innen gleichzeitig verschickt werden, jedoch als Einzelnachricht. So kann nicht jedes Gruppenmitglied alles lesen, auch Telefonnummer und Info werden nicht an andere Gruppenmitglieder geschickt, Antworten der Broadcast-Gruppenmitglieder werden als Einzelnachricht empfangen.
- WhatsApp kann auch als Desktop-Version am Computer oder Laptop verwendet werden.

Die Verwendung von WhatsApp in der Jugendarbeit ist also unter Miteinbeziehung der möglichen Ausnahmefälle eher erlaubt als verboten.

Besonders eine WhatsApp-Gruppe, die auch schon vor dem Inkrafttreten der DSGVO bewährtes Kommunikationsmedium war und immer noch sicherstellt, dass Informationen zu Beratungsangeboten, Veranstaltungen und Aktivitäten gut verbreitet werden können, man bei Verwendung von Alternativen manche Jugendliche sogar verlieren würde, an Reichweite einbüßt, oä., wären Argumente für das Vorhandensein eines berechtigten Interesses. Nichtsdestotrotz wäre der Versuch datenschutzkonforme Ersatzkommunikationsplattformen im Arbeitsumfeld zu etablieren sehr zu begrüßen.

Weiters gilt allgemein die Empfehlung, sensible Gespräche mit Kindern oder Jugendlichen nicht über Messenger-Apps oder Soziale Netzwerke stattfinden zu lassen.

Signal

Die Messenger App Signal wurde von einer gemeinnützigen, spendenfinanzierten Stiftung entwickelt, ist kostenlos, werbe- und trackingfrei. Der Funktionsumfang ist mit WhatsApp vergleichbar. Bilder, Videos, Dokumente und Sprachnachrichten können über Einzel- oder Gruppenchats verschickt werden. Darüber hinaus besteht auch bei Signal die Möglichkeit Videoanrufe zu tätigen.

Rechtliche Grundlagen

- **Signal-Nutzungsbedingungen**: Nutzung ab dem 13. Lebensjahr (oder ab dem im Heimatland vorgeschriebenen Alter) erlaubt.
- **DSGVO in Österreich**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze
- **Die Verwendung von Signal ist DSGVO-konform.** Der Messenger-Dienst arbeitet mit dem sogenannten Zero-Knowledge-Prinzip. Personenbezogene Daten und Profilinformationen werden kryptografisch gehasht, sie werden also in eine individuelle Zeichenkette umgewandelt, nicht in Klarnamen auf den Servern gespeichert und sind so auch für den Messenger-Dienst selbst nicht zuordenbar. Die Absenderadresse wird vor der Übertragung des Inhaltes verschlüsselt, was eine Rekonstruktion der Gesprächspartner*innen unmöglich macht. Daten werden darüber hinaus nicht nur verschlüsselt, sondern auch nur temporär gespeichert.
- **Open Source** (der Programm-Code ist öffentlich einsehbar)
- Jedwede Kommunikation (der Transfer von Bildern, Videos, Textnachrichten, Dateien, Standort und Videoanrufe) ist **Ende-zu-Ende-verschlüsselt.**
- Aufholbedarf besteht lediglich an der Verfügbarkeit der Nutzungsbedingungen bzw. Datenschutzerklärung in sämtlichen Sprachen. Im Moment stehen diese Dokumente nur auf Englisch zur Verfügung, was grundsätzlich nicht dem DSGVO Grundsatz der Transparenz, bzw. dem leichten und verständlichen Zugang zu dienstspezifischen datenschutzrechtlichen Informationen entspricht.

Relevante Funktionshinweise

- Möglichkeit auch die Metadaten geheim zu halten (Einstellung „Vertraulicher Absender“)
- Gruppenchats mit bis zu 150 Personen sind möglich
- Datentransfers bis zu einer Größe von 100 MB sind möglich

Die Verwendung von Signal als Alternative zu anderen Messenger-Diensten und Plattformen, ist auf jeden Fall sehr zu empfehlen.

Telegram

Telegram ist eine kostenlose Messenger-App, mit der, wie auch bei WhatsApp oder Signal, Textnachrichten, Bilder, Videos, Sprachnachrichten und andere Dateien versendet werden können. Eine Registrierung erfolgt über die eigene Telefonnummer. Der Messenger-Dienst kann, ähnlich wie WhatsApp, nicht nur als Smartphone-App, sondern auch im Browser oder als Programm auf dem PC oder Laptop verwendet werden. Die angelegten Chats sind über eine Cloud auf allen Geräten verfügbar. Darüber hinaus ist auch das Telefonieren über Telegram möglich.

Rechtliche Grundlagen

- **Telegram-Nutzungsbedingungen**: Nutzung ab dem 16. Lebensjahr
- Kein Verweis auf ein Herabsetzen der Altersbeschränkung auf Grund länderspezifischer Gesetzeslage. Trotzdem ist davon auszugehen, dass die **Nutzung in Österreich ab dem 14. Lebensjahr** erlaubt ist, wieder ohne rechtliche Konsequenzen für Eltern oder Kinder/Jugendliche bei Nutzung unterhalb der erlaubten Altersgrenze
- **Die DSGVO konforme Nutzung von Telegram ist nach momentanem Stand der Datenschutzrichtlinien zu verneinen.** Die Datenschutzerklärung steht auch bei Telegram nur auf Englisch zur Verfügung, was dem DSGVO-Grundsatz der Transparenz, bzw. dem leichten und verständlichen Zugang zu dienstspezifischen datenschutzrechtlichen Informationen widerspricht.

  Im Gegensatz zu Signal werden bei Telegram jedoch IP-Adresse, Nutzername und Informationen über die App-Version für 12 Monate gespeichert, ohne jedoch den genauen Zweck dafür anzugeben. Unklar ist darüber hinaus auch der Umgang mit Standortdaten und offenen Chats.

  Laut Nutzungsbedingungen werden Kontaktdaten, nach erlaubtem Zugriff auf verschiedenen „Servern rund um die Welt“ gespeichert, der genaue Standort wird nicht bekanntgegeben.

  Hinter Telegram steckt zudem ein sehr undurchsichtiges Firmengeflecht, was es unmöglich macht genau herauszufinden, was schlussendlich mit gesammelten Informationen und Daten passiert.

Relevante Funktionshinweise

- Kostenloses Service, Quellcode ist aber nur zum Teil öffentlich einsehbar.
- **Chats sind nicht standartmäßig Ende-zu-Ende-verschlüsselt**, nur in der Funktion „Geheimer Chat“ ist diese Sicherheitsfunktion gegeben.
- Die Ende-zu-Ende-Verschlüsselungsfunktion ist nicht auf Gruppenchats anwendbar.
- Telegram bietet die Funktion im geheimen Chat, dass Nachrichten nach einer gewissen Zeit (Einstellungsmöglichkeiten 1-30 Sek.,1 Min., 1h, 1 Tag, 1 Woche) automatisch gelöscht werden.
- Datentransfer bis zu einer Größe von 1,5 GB ist möglich
- Telegram-Gruppenchats mit bis zu 200.000 Teilnehmer*innen sind möglich
- Telegram bietet im Moment noch keine Möglichkeit Videoanrufe zu tätigen.

Die Verwendung von Telegram als Kommunikationsmittel bzw. Ersatz für WhatsApp ist unter Berücksichtigung der Existenz datensparsamerer, transparenterer und DSGVO konformer Alternativen, nicht zu empfehlen.

Instagram

Instagram ist eine kostenlose App zum Teilen von Fotos und Videos, die gleichzeitig auch in anderen Sozialen Netzwerken geteilt werden können (z. B. Facebook, Twitter oder Tumblr). Es besteht die Möglichkeit Inhalte vor der Veröffentlichung direkt in der App zu bearbeiten bzw. mit Filtern zu versehen. Darüber hinaus werden geteilte Inhalte oft mit sogenannten Hashtags (Doppelkreuz = Raute = Hashtag = #) versehen. Hashtags sind eine Art Verlinkung, welche anderen Nutzer*innen weitere Fotos mit demselben Hashtag anzeigt. Darüber hinaus besitzt Instagram mit **IGTV** eine eigene interne Videoplattform. Über mobile Geräte können Videos mit einer Länge zwischen einer und 15 Minuten hochgeladen werden, über das Web sogar Videos mit einer Länge bis zu einer Stunde. Weiters besteht die Möglichkeit auch Nachrichten, Bilder, Videos, Sticker oder Sprachnachrichten an Nutzer*innen über das in die Plattform integrierte Service **Istagram Direct Message** zu verschicken. Instagram kann auch am PC genutzt werden, jedoch lassen sich die meisten Funktionen (wie z.B. Bilder und Videos hochladen) nur in der App ausführen. Andere Funktionen, wie z.B. das Löschen des Kontos kann wiederum nur in der Desktop-Version getätigt werden.

Rechtliche Grundlagen

- **Instagram-Nutzungsbedingungen**: Nutzung grundsätzlich ab dem 13. Lebensjahr erlaubt, bzw. auch von jüngeren, sofern im Steckbrief angeben ist, dass das Konto von einem Elternteil oder Manager verwaltet wird (Stichwort „Sharenting“).
- **DSGVO Österreich**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze

Welche Daten werden gesammelt?

- Nutzerdaten, wie Benutzername, E-Mail-Adresse, aber auch – falls man diese angibt – die Telefonnummer und den echten Namen.
- Bei der Instagram-Nutzung anfallende Daten, also eigene Fotos, Videos, Stories sowie Informationen darüber, welche Inhalte anderer man ansieht, die Zeit, Häufigkeit und Dauer der Aktivitäten, die Kommentare, Likes und **Inhalte der Direct Messages**.
- Der Aufnahmestandort eines Fotos.
- Sämtliche Informationen, die man im Profil angibt oder die sich aus den Posts ergeben, z.B. politische Ansichten, die Religion oder die Sexualität, was nach **Art. 9 DSGVO** zu den **sensiblen Daten** zählt.
- Informationen über die Personen, Seiten, Konten sowie Hashtags, mit denen man sich verbindet und wie mit diesen interagiert wird.
- Kontaktinformationen aus dem Adressbuch, Anrufprotokoll oder der SMS-Protokollhistorie, wenn diese vom jeweiligen verwendeten Gerät hochgeladen, synchronisiert oder importiert werden.
- Von anderen Nutzern hochgeladene Fotos und Videos, auf denen man zu sehen ist sowie deren Kommentare unter dem eigenen Foto.

- Informationen über Social Plugins, APIs, SDKs und Facebook Pixel, also z.B. zum Gerät, den besuchten Websites, den getätigten Käufen, den gesehenen Werbeanzeigen und zur Nutzung der Dienste – unabhängig davon, ob man ein Instagram-Konto hat oder eingeloggt ist.
- Informationen zum verwendeten Gerät, also z.B. das Betriebssystem, die Signalstärke, der verfügbare Speicherplatz, der Browsertyp, die App- und Dateinamen, sowie Mausbewegungen, die Geräte-ID, WLAN-Zugangspunkte und Funkzellentürme in der Nähe.
- Falls der Zugriff gestattet wurde, der GPS-Standort
- Und die Mobiltelefonnummer sowie die IP-Adresse.

Die Verwendung des intern angebotenen Nachrichtendienst „Instagram Direct Message“ (besonders für berufliche Zwecke) als Kommunikationsmedium ist nicht datenschutzkonform, da keine Ende-zu-Ende-Verschlüsselung besteht, versendete Inhalte für Werbezwecke analysiert, bzw. teils sensible Daten ausgewertet werden. Die Verwendung als Kommunikationstool ist nicht empfehlenswert.

Snapchat

Snapchat ist ein kostenloser Messenger für Smartphones und Tablets zum Versenden von Text- oder Sprachnachrichten, Fotos und Kurzvideos ("Snaps"). Eine Besonderheit dieses Messenger-Dienstes ist die Möglichkeit, der/dem Empfänger*in die Inhalte nur für kurze Zeit zur Verfügung zu stellen, nach 1-10 Sekunden verschwinden die Bilder oder Kurzvideos aber wieder von selbst. Die Fotos und Videos werden direkt in der App erstellt und können mit vielen Extras (z.B. Text, Emojis...) versehen oder mit speziellen Augmented Reality[6] Filtern bearbeitet werden. Snapchat wird gern dazu genutzt, besonders "blöde" oder freizügige Fotos zu verschicken.

Rechtliche Grundlagen

- **Snapchat Nutzungsbedingungen**: Verwendung ab dem 13. Lebensjahr erlaubt, bzw. ab dem Alter, das vonnöten ist, um rechtsverbindliche Verträge abschließen zu können. Darüber hinaus gilt es auf lokale, nationale, landesspezifische sowie internationale Gesetze Rücksicht zu nehmen. Verurteilte Sexualstraftäter sind von der Nutzung ausgeschlossen.
- **DSGVO in Österreich**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze.

Welche Daten werden gesammelt?

- Informationen über die Tätigkeit des Users, Nachrichten, die er über den Service sendet und empfängt.
- Uhrzeit, Datum, Absender, Empfänger einer Nachricht.
- Anzahl der Nachrichten, die der User mit Ihren Freunden austauscht.
- Geräteinformationen, z.B. Hardware-Modell, Betriebssystem, Gerätekennungen, Sprache, Telefonnummer des Mobilgerätes und Informationen zum Mobilnetzwerk.
- Informationen aus dem Telefonbuch.
- Infos zu Fotos auf dem Gerät.
- Standortinformationen.

Laut Nutzungsbedingungen werden Inhalte von Nachrichten nicht länger gespeichert als nötig, also nur bis zur erfolgreichen Übertragung. Bis dorthin hat Snapchat jedoch uneingeschränkten Zugriff auf sämtliche Informationen. Der Messenger-Dienst nimmt weiters auch das Recht heraus, bei der Aufklärung von Straftaten belastende Inhalte ermittelnden Behörden zur Verfügung zu stellen. Die Übermittlung von Inhalten über diesen Messenger-Dienst erfolgt nicht auf Ende-zu-Ende-verschlüsseltem Weg.

Eine datenschutzkonforme und damit rechtlich zulässige Verwendung der Snapchat-Nachrichtenfunktion ist keinesfalls möglich.

[6] „Erweiterte Realität“. Auf ein analoges Live-Porträt wird zum Beispiel ein virtueller Hut projiziert.

TikTok

TikTok ist eine App des chinesischen Konzerns ByteDance, mit der 15-sekündige bis 5-minütige Musikvideos aufgenommen und mit anderen Nutzer*innen geteilt werden können. Die Nutzer*innen singen dabei nicht selbst, sondern können aus einer umfangreichen Datenbank Lieder, Film- oder Serienszenen auswählen und dazu ihre eigene Playback-Show mit Tanzeinlagen oder Lippensynchronisation gestalten. Die Videos werden in weiterer Folge mit Spezialeffekten, Filtern oder Stickern bearbeitet und mit passenden Hashtags versehen, um die Reichweite der Fans (=Follower) zu erweitern. Ein Hashtag definiert dabei eine bestimmte Kategorie und erleichtert das Finden von Videos derselben Kategorie. Auch TikTok bietet eine eigene Nachrichtenfunktion innerhalb der Plattform, worüber jedoch lediglich Textnachrichten verschickt werden können.

Rechtliche Grundlagen

- **TikTok-Nutzungsbedingungen**: Die Nutzung ist ab dem 13. Lebensjahr erlaubt, jedoch bis zum 18. Lebensjahr nur mit offizieller Einwilligung eines Erziehungsberechtigten.
- **DSGVO in Österreich**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze.

Welche Daten werden gesammelt?

- Bei der Registrierung Name, E-Mail-Adresse, Telefonnummer, Fotos, Sprachauswahl
- Nutzungsverhalten wird aufgezeichnet (Likes, Kommentaren, **sogar Inhalte von privaten Nachrichten**)
- Laut offizieller Datenschutzerklärung dürfen auch Daten außerhalb der Plattform gesammelt werden
  - Browserverlauf
  - Mobilfunkanbieter, Zeitzone und lokale Einstellungen
  - Daten, die man in anderen sozialen Netzwerken teilt, zum Beispiel Facebook

Es ist darüber hinaus nicht nachvollziehbar, wo die Aufbewahrung der Daten erfolgt bzw. wer die Daten tatsächlich erhält. In den Nutzungsbedingungen wird lediglich erwähnt, dass gesammelte Informationen an Geschäftspartner, Service-Provider und innerhalb des Konzerns weitergegeben werden können und außerhalb des Europäischen Wirtschaftsraumes verarbeitet werden. Das würde bedeuten, dass über 4.500 Partnerunternehmen, die mit ByteDance wirtschaftlich verbunden sind, Zugriff auf teils personenbezogene Daten hätten. Weiters häufen sich Berichte, dass TikTok bestimmte Inhalte zensiere, besonders wenn es um chinesische Regimekritik geht.

Eine datenschutzkonforme Verwendung der Plattform TikTok ist somit absolut unmöglich.

Facebook Messenger

Der Facebook-Messenger ist eine kostenlose App zum Empfangen und Versenden von Facebook-Nachrichten auf dem Smartphone. Neben dem Versenden von Nachrichten, Fotos, Videos, Stickern und Sprachnachrichten, kann der Messenger auch für Videoanrufe verwendet werden.

Rechtliche Grundlagen

- **Facebook Nutzungsbedingungen**: Nutzung des Messengers ist ab dem 13. Lebensjahr erlaubt
- **DSGVO in Österreich**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze
- Voraussetzung für die Nutzung ist entweder ein Facebook-Profil, bzw. die Angabe der Telefonnummer
- Nachrichten sind nicht standartmäßig Ende-zu-Ende-verschlüsselt, eine Verschlüsselung kann jedoch bei einer Unterhaltung mit nur einer Person aktiviert werden. Diese Zusatzfunktion ist nicht bei Gruppenchats anwendbar.

Welche Daten werden gesammelt?

- Name[7] und Standort der Nutzer*innen, sofern man die Ortungsfunktion nicht deaktiviert hat.
- Facebook macht nur sehr vage Angaben darüber, in welchem Umfang Daten bei Verwendung des Messengers gesammelt werden. In der Datenschutzerklärung ist lediglich davon die Rede, dass „Inhalte, Kommunikationen und sonstige Informationen" erfasst und für personalisierte, auf Nutzerinteressen zugeschnittene Werbung verwendet werden.
- Bei verschlüsselten Chats werden die anfallenden Metadaten gespeichert und ausgewertet (z.B. mit welchem Chatkontakt wie oft und wie lange über welches Gerät kommuniziert wird).
- Alle aus- und eingehenden, auch verschlüsselten Nachrichten werden standardmäßig, zur Verhinderung von Straftaten, auf Schlüsselwörter überprüft.

Einer Verwendung des Facebook-Messengers als Kommunikationsmedium in der Arbeit mit Zielgruppen ist auf jeden Fall abzuraten.

[7] Seit Ende 2019 besteht keine Klarnamenpflicht mehr auf Facebook, bzw. allen dazugehörigen Diensten.

Discord

Discord ist eine kostenlose[8] App für Chats, Übertragungen von Bildern, Videos, Dateien sowie Sprach- und Videokonferenzen, die sowohl auf mobilen Endgeräten wie dem Smartphone oder dem Tablet als auch am Computer verwendet werden kann.

Jeder Discord-Nutzer kann eigene Server erstellen, um sich mit Freunden oder Gleichgesinnten sozusagen in Gruppen-Chats zu einem speziellen Thema auszutauschen. Ein Server bietet die Möglichkeit – wie in einem eigenen kleinen sozialen Netzwerk – Text- und Sprachkanäle sortiert nach verschiedenen Themen für andere zur Verfügung zu stellen. So kann jede*r schnell zum Sender oder zur Senderin eigener Inhalte werden und kontrollierbare Räume zur Kommunikation mit anderen schaffen.

Die Erstellung solcher Server ist bei vielen anderen Plattformen (z.B. TeamSpeak oder Slack) kostenpflichtig, wohingegen Discord den dafür benötigten Webspace kostenlos zur Verfügung stellt. Außerdem sind viele Jugendliche bereits auf Discord unterwegs, kennen die Logik und Anwendungsbereiche der Plattform und sind schnell für die Nutzung zu begeistern.

Rechtliche Grundlagen

- **Discord Nutzungsbedingungen**: Nutzung ist ab dem 13. Lebendjahr erlaubt.
- **DSGVO in Österreich**: Nutzung ab dem 14. Lebensjahr erlaubt, jedoch keine rechtlichen Konsequenzen bei Nutzung unterhalb der erlaubten Altersgrenze.

Welche Daten werden gesammelt?

- Benutzername, E-Mail-Adresse
- Alle Nachrichten, Bilder, und andere Inhalte, die über die Chat-Funktion verschickt werden
- IP-Adresse, Geräte-ID und Aktivitäten innerhalb der Dienste
- Daten aus mit Discord verbundenen Sozialen Netzwerken
- Daten dürfen mit Tochtergesellschaften, Agenturen und Geschäftspartnern geteilt werden

Discords Datenschutzbestimmungen entsprechen bei weitem nicht unseren Datenschutzanforderungen hinsichtlich DSGVO. Daher gilt es sorgsam abzuwägen, ob der Einsatz von Discord in der Arbeit mit Kindern und Jugendlichen als pädagogisches Werkzeug gewollt ist. Eine Abstimmung mit Arbeitgebern bzw. Datenschutzbeauftragten, mit Rücksichtnahme auf gegebenenfalls schon getroffene Vereinbarungen und ausgearbeitete Richtlinien zur Nutzung anderer Plattformen, ist jedenfalls erforderlich. Der Einsatz von Discord in der Kinder- und Jugendarbeit sollte somit nur unter ausführlicher Abwägung des Datenschutzes gegenüber dem pädagogischen Nutzen und unter Berücksichtigung wichtiger Aspekte des Jugendschutzes stattfinden.

[8] Discord stellt alle Basisfunktionen gratis zur Verfügung. Für verbesserte Sprach- und Bildqualität bzw. kosmetische Einstellungsmöglichkeiten mithilfe von Emojis oder speziellen Icons, bietet Discord zwei Abo-Varianten, Discord Nitro (10€ im Monat) und Discord Nitro Classic (5€ im Monat).

Anhang

Allgemein

- https://www.sos-kinderdorf.at/getmedia/123fef25-f426-4858-9f58-00867954f847/2018-09-Digitale-Medien,-online-Version_1.pdf
- https://www.saferinternet.at/news-detail/mindestalter-ab-wann-duerfen-kinder-whatsapp-instagram-co-nutzen/#:~:text=Wie%20das%20in%20der%20Praxis,nicht%20mit%20Facebook%20verkn%C3%BCpft%20ist.

WhatsApp

Nutzungsbedingungen

- https://www.whatsapp.com/legal/?lang=de&eea=0
- https://www.handysektor.de/artikel/dein-vertrag-mit-whatsapp

Datenschutzrichtlinie
https://www.whatsapp.com/legal/privacy-policy

Privatsphäre Leitfaden
https://www.saferinternet.at/privatsphaere-leitfaeden/whatsapp/

WhatsApp Verwendung in der Jugendarbeit

- https://www.saferinternet.at/faq/jugendarbeit/duerfen-jugendarbeiterinnen-weiterhin-whatsapp-verwenden-um-mit-jugendlichen-in-kontakt-zu-bleiben/
- https://www.derstandard.at/story/2000080991460/darf-mein-kind-eigentlich-whatsapp-nutzen

Signal

Nutzungsbedingungen

- https://signal.org/legal/#terms-of-service
- https://www.handysektor.de/artikel/dein-vertrag-mit-signal

Datenschutzerklärung
https://signal.org/legal/#privacy-policy

Telegram

Datenschutzerklärung
https://telegram.org/privacy

Relevante Informationen des Anbieters
https://telegram.org/faq

Instagram

Nutzungsbedingungen

- https://help.instagram.com/581066165581870
- https://www.handysektor.de/artikel/dein-vertrag-mit-instagram

Datenschutzerklärung
https://help.instagram.com/519522125107875

Privatsphäre Leitfaden
https://www.saferinternet.at/privatsphaere-leitfaeden/instagram/

Snapchat

Datenschutzerklärung
https://www.snap.com/de-DE/privacy/privacy-policy/

Nutzungsbedingungen

- https://www.snap.com/de-DE/terms
- https://www.handysektor.de/artikel/dein-vertrag-mit-snapchat

Privatsphäre Leitfaden
https://www.saferinternet.at/privatsphaere-leitfaeden/snapchat/

TikTok

- https://fm4.orf.at/stories/2998463/
- https://netzpolitik.org/2019/gute-laune-und-zensur/

Datenschutzerklärung
https://www.tiktok.com/legal/privacy-policy?lang=de

Privatsphäre Leitfaden
https://www.saferinternet.at/privatsphaere-leitfaeden/tiktok/

Discord

Datenschutzerklärung
https://support.discord.com/hc/de/articles/360004109911-Datenschutzbestimmungen

Nutzungsbedingungen
https://discord.com/terms

Videokonferenz plattformen

Rechtliche Grundlagen und relevante Funktionshinweise

Bedingt durch die Coronavirus-Pandemie und die damit verbundenen Einschränkungen des öffentlichen Lebens und persönlicher Kontakte, war ein Aufrechterhalten vorhandener Strukturen und Arbeitsabläufe nur durch eine Verlagerung der Kommunikation auf bereits vorhandene Online-Dienste möglich. Der explosionsartige Anstieg der Nutzerzahlen erforderte (und erfordert immer noch) rasche Reaktionen auf technische Mängel und Anpassungen rechtlicher Rahmenbedingungen seitens der Anbieter.

Die österreichische Datenschutzbehörde hat betreffend Rechtmäßigkeit und dem Level technischer Standards bisher noch kein Statement abgegeben, was einen Blick nach Deutschland und eine sehr umfangreiche Recherche unumgänglich machte. Die 16 in Deutschland ansässigen Datenschutzbehörden teilen, den Themenblock Videokonferenzsysteme betreffend, jedoch sehr unterschiedliche Rechtsmeinungen, bzw. herrscht auch unter (Datenschutz-) Expert*innen im deutschsprachigen Raum alles andere als Konsens in Hinblick auf rechtmäßigen Einsatz gängiger Videokonferenzplattformen.

Besonders hervorzuheben sind hierbei die sehr kontroversen Stellungnahmen der Berliner Beauftragten für Datenschutz und Informationsfreiheit von Mai 2020 und Februar 2021, die besonders den großen Anbietern ein schlechtes Zeugnis ausstellt und eine rechtskonforme Verwendung von Zoom, MS Teams und Cisco Webex, trotz Bemühungen und vertraglicher Adaptionen ausschließt, ohne dabei auf technische Aspekte wie zum Beispiel Ende-zu-Ende-Verschlüsselungen, Server-Standortauswahl, zusätzliche Datenschutz-Einstellungsmöglichkeiten, etc. Bezug zu nehmen. Darüber hinaus gab es mit dem EuGH-Urteil Schrems II und der damit Verbundenen Auflösung des Privacy Shield Abkommens zwischen der Europäischen Union und den USA von 16. Juli 2020 tiefgreifende Veränderungen betreffend Datentransfer und rechtskonformer Verwendung amerikanischer IT-Dienstleistungen.

Die vorliegende Nutzenabwägung ist eine Momentaufnahme und eine Zusammenfassung der aktuellen Lage (Stand März 2021), unter Berücksichtigung rechtlicher und technischer Aspekte, mit besonderem Augenmerk auf Verschlüsselung und datenschutzrelevanten vertraglichen Rahmenbedingungen wie EU-Standardvertragsklauseln und Auftragsverarbeitungsvertrag.

Zoom

Verglichen mit den anderen Videokonferenzanwendungen, war wohl keine der Plattformen so stark medialer Kritik ausgesetzt wie Zoom. Hauptgrund dafür war das Explodieren der Nutzer*innenzahlen zu Beginn des letzten Jahres (von 10 Mio. auf 300 Mio. Nutzer*innen weltweit innerhalb von 90 Tagen[9]), die damit verbundene Erweiterung des Klientels und der Umstand, dass Zoom für kleine und mittelgroße Teams in Unternehmen konzipiert wurde, nicht jedoch für den Bildungssektor oder die private Anwendung. Mit diesem Konzept der einfachen Nutzbarkeit in Unternehmensstrukturen, waren anfänglich zahlreiche Sicherheitslücken und Datenschutzbedenken verbunden. Zoom bietet in der Gratisversion Meetings mit bis zu 100 Teilnehmer*innen über eine Dauer von maximal 40 Minuten. Darüber hinaus können zahlreiche verschiedene Lizenzen erworben werden, um den Funktionsumfang zu erweitern.

Kriterien

Zoom stand besonders auf Grund des Phänomens *Zoombombing* stark in der Kritik. Besondere Aufmerksamkeit erregten Vorfälle an New Yorker Schulen, wo schulfremde Personen Kenntnis der 9-stelligen Meeting-ID erlangten, in virtuelle Klassenräume eindrangen und dort ungeeignete Inhalte teilten[10].

Mittlerweile sind Zoom-Meetings automatisch gesichert, entweder durch einen Passcode, eine Wartraum-Funktion oder eine Authentifizierung der Teilnehmer*innen vor Eintritt in den Raum. Wählt der Gastgeber der Veranstaltung keine der Sicherheitsoptionen aus, erstellt das Programm automatisch einen Warteraum und der Host darf entscheiden wer eintreten darf. Das Teilen von Bildschirmen für Teilnehmer*innen wurde deaktiviert und Räume können, zusätzlich zu den anderen Sicherheitsmöglichkeiten, nach Eintritt aller geladenen Gäste gesperrt werden.

Verschlüsselung

Kritik gab es auch an der Verschlüsselung allgemein bzw. an der Verschlüsselung der Meetings, die bis zur Version 5.4.0 aus einer Transportverschlüsselung bestand.
Demnach war nur der Weg zwischen Server und Client verschlüsselt, Daten auf den Servern konnten theoretisch eingesehen werden.

Sehr rasch wurde die Verschlüsselung auf einen AES 256-bit GCM Standard gesetzt, der allgemein als sehr sicher gilt. Darüber hinaus besteht seit Oktober 2020 die Möglichkeit Meetings Ende-zu-Ende zu verschlüsseln. Diese Funktion muss in den Einstellungen[11] aktiviert werden und entspricht den Sicherheitsstandards verschlüsselter Messaging-Dienste[12]. Weitere Voraussetzung ist eine aktuelle Version des Videokonferenztools[13].

[9] https://blog.zoom.us/90-day-security-plan-progress-report-april-22
[10] https://thenextweb.com/security/2020/04/06/nyc-classrooms-cancel-zoom-after-trolls-make-zoombombing-a-thing/
[11] Anmelden auf der Zoom-Website / Links im Menü *Kontoverwaltung* / *Kontoeinstellungen* / *End-to-End Verschlüsselung nutzen* aktivieren
[12] https://blog.zoom.us/de/zoom-rolling-out-end-to-end-encryption-offering/
[13] Mindestens Version 5.4.0

Datenschutz

Der Unternehmenssitz von Zoom befindet sich in den Vereinigten Staaten von Amerika. Der Datenverkehr wurde vor allem über zugemietete Server aus den USA und China geleitet, was bezüglich DSGVO häufig kritisiert wurde. Laut dieser dürfen personenbezogene Daten nur außerhalb des Europäischen Wirtschaftsraumes verarbeitet werden, wenn der Europäische Datenschutzausschuss dem Drittland ein äquivalentes Datenschutzniveau ausgestellt hat, was zum Beispiel für die Schweiz, Kanada oder Neuseeland, nicht ohne weiteres aber für die USA gilt. Bis Juli 2020 war für einen DSGVO-konformen Austausch die EU-USA Privacy Shield Registrierung erforderlich[14][15]. Dieses Abkommen wurde jedoch vom EuGH am 16. Juli 2020 für rechtswidrig und damit unwirksam erklärt. Zoom unterliegt als amerikanischer IT-Dienstleister auch dem sogenannten CLOUD Act[16] und ist demnach unter gewissen Umständen verpflichtet, Daten an US-Behörden auszuhändigen, auch wenn diese im Ausland gespeichert werden.

Gegen die Herausgabe von Daten, die in einem EU-Mitgliedstaat gespeichert werden, besteht laut diesem Gesetz aber ein besonderes Widerspruchsrecht,
wenn es sich beim Eigentümer der Daten nicht um einen amerikanischen Staatsbürger handelt, der Hauptwohnsitz außerhalb des US-Staatsgebietes liegt und die Herausgabe der Daten gegen andere geltende Gesetze (wie etwa die DSGVO) verstoßen würde. Besitzer eines Zoom Pro-, Business-, Enterprise oder Bildungskontos haben die Möglichkeit in den Einstellungen auszuwählen, über welche Serverstandorte der Datenverkehr der Meetings oder Webinare laufen soll. [17]

Weiters wurde der bei der Registrierung automatisch abgeschlossene Auftragsdatenverarbeitungsvertrag um EU-Standartvertragsklauseln und um die Möglichkeit erweitert, Meetings und Webinare Ende-zu-Ende-verschlüsselt durchzuführen.[18] Damit folgte man der Empfehlung des Europäischen Datenschutzausschusses zusätzlich zu vertraglichen Veränderungen auch technische Schutzmechanismen zu installieren. Für den Fall, dass nur zwei Teilnehmer*innen miteinander kommunizieren, schaltet Zoom automatisch auf eine sogenannte Peer-to-Peer-Verbindung um. Der Datenverkehr findet damit direkt ohne Verbindung zu den Zoom-Servern statt.

[14] Dem Urteil des EuGHs ging eine Klage des österreichischen Datenschutzaktivisten Max Schrems voraus.
[15] Zoom ist registriertes Mitglied.
[16] Der **C**larifying **L**awful **O**verseas **U**se of **D**ata Act ist ein Gesetz, das US-Internetfirmen und IT-Dienstleister dazu verpflichtet, amerikanischen Behörden auf Verlangen, meist zum Zwecke der Strafverfolgung, Zugriff auf Daten zu gewähren, auch wenn diese im Ausland gespeichert werden. Microsoft zählt zu den größten Kritikern dieses Gesetzes.
[17] Anmelden auf der Zoom-Website / Links im Menü *Kontoverwaltung* / *Kontoeinstellungen / Select data center regions for meetings/webinars hosted by your account* aktivieren und Serverstandorte auswählen/deaktivieren.
[18] Gemäß Art. 46 Abs.2 lit. C (nach Abschluss des Prüfverfahrens nach Art. 93 Abs. 2) eine geeignete Garantie, die Übermittlung personenbezogener Daten an Drittstaaten rechtmäßig durchführen zu können.

Nutzungsempfehlung

Zoom hat auf die anfänglich berechtigte Kritik sehr schnell reagiert und versorgt Nutzerinnen und Nutzer ständig mit neuen Updates. Im direkten Vergleich mit anderen Plattformen, liefert Zoom die benutzerfreundlichste Oberfläche und einfachste Bedienung. Weiters punktet Zoom mit einer stabilen Video- und Tonverbindung auch bei geringer Internetbandbreite und hoher Teilnehmer*innenzahl, sowie der Möglichkeit der Verwendung auf Smartphones und Tablets. Darüber hinaus stehen nützliche Tools wie Breakout Sessions, Whiteboard oder Umfragen zur Verfügung und es werden bis zu 49 Videos gleichzeitig auf dem Bildschirm gezeigt, was besonders die Arbeit mit größeren Gruppen erleichtert. Nach Erweiterung des Auftragsdatenverarbeitungsvertrages durch EU-Standardvertragsklauseln bzw. der Einführung der Ende-zu-Ende-Verschlüsselung bei Meetings und Webinaren, ist eine DSGVO-konforme Nutzung auf jeden Fall möglich. Voraussetzung dafür ist allerdings eine bezahlte Version der Plattform, da viele der relevanten Einstellungsmöglichkeiten in der Gratisversion nicht zur Verfügung stehen.

MS Teams

Die Videokonferenzplattform, die zur Microsoft 365 Familie gehört, zählt, besonders in Hinblick auf Nutzer*innenzahlen, sicherlich auch zu den Gewinner*innenn der Coronakrise. Die Zahl der täglich aktiven Nutzer*innen hat sich innerhalb des letzten Jahres mehr als verdoppelt (45 Mio. im März 2020 → 115. Mio im Dezember 2020), was einen rapiden Ausbau der Server- und IT-Landschaften innerhalb kurzer Zeit bzw. eine Nachbesserung von Funktionen und Nutzungsbedingungen nötig machte.

Kriterien

Verschlüsselung

Die Verschlüsselung der Daten auf dem Weg von Server zu Server, Client zu Server, die Enkodierung der Medienflüsse bzw. der Audio- und Videofreigaben erfüllt hohe Sicherheitsstandards. Angriffe von außerhalb sind dadurch (laut eigenen Angaben) sehr schwierig bis unmöglich[19]. Im Gegensatz zu Zoom besteht jedoch nach heutigem Stand keine Möglichkeit, Online-Meetings und Webinare mit einer Ende-zu-Ende-Verschlüsselung zu versehen. Das eröffnet die theoretische Möglichkeit, gespeicherte Daten auf den Microsoft-Servern einzusehen bzw. Informationen auf Grund geltender Gesetze (Cloud Act) unverschlüsselt weiterzugeben. Microsofts Lösung hierzu ist ein Zwei-Schlüssel-System für alle in Microsoft 365 integrierten Programme (also auch MS Teams). Alle Daten werden hierbei doppelt verschlüsselt, wobei ein Schlüssel bei Microsoft, der andere bei der Nutzerin oder dem Nutzer bleibt. Ohne beide Schlüssel, so die Erklärung von Microsoft, ist eine Einsichtnahme in Daten auch für Behörden keinesfalls möglich.

Datenschutz

Mediale Kritik den Datenschutz betreffend gab es auch in Richtung MS Teams. Die Berliner Beauftragten für Datenschutz und Informationsfreiheit veröffentlichten im Mai letzten Jahres eine Stellungnahme zum Einsatz von Microsoft-Videokonferenzsystemen (die eine Microsoft 365 Lizenz voraussetzen) mit dem Ergebnis, dass MS Teams nicht datenschutzkonform verwendet werden könne.

Diese Einschätzung wird jedoch von zahlreichen Expert*innen und auch innerhalb des Gremiums kritisiert, da sich die Berliner Behörde weder zu tatsächlich stattfindenden Verarbeitungen personenbezogener Daten und der damit einhergehenden Datenschutzkonformität noch zu technischen Aspekten äußert. Weiters wurden bereits erfolgte Adaptionen des Vertragswerkes außer Acht gelassen und auf veraltete Versionen der Standardverträge Bezug genommen. Auch im aktuellen Statement von 18.02.2021 wird besonderes Augenmerk auf Regelungen im sogenannten Data Processing Agreement (DPA) und den darin enthaltenen Vertragsklauseln zum Datenaustausch der Europäischen Microsoft-Tochtergesellschaft mit dem amerikanischen Mutterkonzern gelegt, die nach Prüfung der Behörde, insbesondere auf Grund der gesetzlichen Verpflichtung zur Herausgabe von Daten auf Grund des CLOUD Acts, nicht den Vorgaben der DSGVO entsprechen.

[19] https://docs.microsoft.com/de-de/microsoftteams/teams-security-guide

Microsoft hat sehr rasch (auch auf Empfehlungen des Europäischen Datenschutzausschusses[20]) reagiert und sich vertraglich dazu verpflichtet, Kunden finanziell zu entschädigen, sollte Microsoft einer staatlichen Stelle unter Verletzung der DSGVO Daten zur Verfügung stellen. Ein weiterer Punkt der Verpflichtung beinhaltet, dass sie *„[…] jede Anfrage einer staatlichen Stelle – egal von welcher Regierung – nach Daten unserer Unternehmenskunden oder unserer Kunden aus dem öffentlichen Sektor anfechten werden, wenn es dafür eine rechtliche Grundlage gibt*."[21]

Bei den anderen von der Berliner Behörde bemängelten Vertragsklauseln handelte es sich um Übersetzungsfehler bzw. mangelnde Genauigkeit in der Formulierung, die ebenso sehr schnell behoben wurden. Obendrein wurde auch die DPA um EU-Standartvertragsklauseln erweitert und damit eine durchaus taugliche rechtliche Grundlage für den Datenaustausch geschaffen. Manche Expert*innen erachten auch diese Änderungen nicht für ausreichend und beziehen sich dabei auf den Wortlaut der Empfehlung des Europäischen Datenschutzausschusses, der als zusätzlichen Schritt, um ein ausreichendes Datenschutzniveau gewährleisten zu können auch technische Maßnahmen anführt, was Microsoft mit der oben erwähnten 2 Schlüssel-Lösung umzusetzen versucht. Weiters bietet auch MS Teams die Möglichkeit Serverstandorte auszuwählen, vor ungebetenen Gästen bei Meetings schützt eine Warteraumfunktion.

Nutzungsempfehlung

MS Teams bietet zusätzlich zur Videokonferenzfunktion die Möglichkeit der virtuellen Zusammenarbeit. So kann die Plattform mit allen Office-Anwendung und darüber hinaus mit bis zu 250 zusätzlichen Apps verbunden werden. Datenaustausch, Möglichkeit der kooperativen Bearbeitung von Dokumenten und Zugriffsmöglichkeit von mobilen Geräten wie Tablets und Smartphones, machen MS Teams zu einem wichtigen Unterstützer von Arbeitsabläufen in Zeiten von Homeoffice und Kontaktbeschränkungen.

MS Teams wurde (wie auch Zoom) im Bericht der Berliner Datenschutzbehörde vom 18.02.2021 nach Prüfung des Vertragswerkes mit einer roten Ampel versehen. Eine DSGVO-konforme Nutzung ist demnach nicht möglich, Anpassungen der Vertragsklauseln sind jedenfalls erforderlich. Die Prüfung wurde allerdings nicht auf technische Datenschutzeinstellungsmöglichkeiten erweitert.

Datenschutzexpert*innen anderer Institutionen sind der Meinung, dass gerade technische als auch organisatorische Vorkehrungen eine rechtskonforme Durchführung von Webinaren und Online-Konferenzen über MS Teams möglich machen.

Daten von Nutzer*innen können beispielsweise pseudonymisiert werden, in den Einstellungen findet sich die Option europäische Server für die Datenübertragung auszuwählen, es besteht immer die Möglichkeit im Vorfeld Einwilligungserklärungen der Nutzer*innen einzuholen, bzw. besteht die Möglichkeit das Sammeln von Meta- und Diagnosedaten in den Einstellungen gänzlich zu unterbinden. Mit etwas Aufwand ist demnach auch eine rechtskonforme Verwendung von MS Teams möglich.

[20] https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_de

[21] https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten/

Skype for Business online

Die genaue Betrachtung dieser Videokonferenzplattform ist nicht vonnöten, da der Dienst mit 31.07.2021 vollständig in MS Teams integriert wird und ab diesem Zeitpunkt nicht mehr eigenständig zur Verfügung steht.

Cisco WebEx

Webex ist das Tochterunternehmen des US-Telekommunikationskonzerns Cisco Systems, Inc. In der kostenlosen Version des Dienstes können bis zu 100 Teilnehmer*innen zusammenfinden, innerhalb des Unternehmens ist die Nutzung auf 90 Tage beschränkt. Teilnehmende können über einen Link einsteigen lediglich der Gastgeber benötigt einen WebEx-Account. Mit der Bezahlversion des Dienstes erhöht sich der Cloudspeicher bzw. auch die maximale Teilnehmer*innenzahl auf bis zu 1000. Darüber hinaus besteht die Möglichkeit nur Audioanrufe zu tätigen, Drittanbieteranwendungen einzubinden, Dateien auszutauschen, über ein Whiteboard gemeinsam zu arbeiten oder Teilnehmende in Kleingruppen aufzuteilen (Breakout Sessions).

Kriterien

Verschlüsselung

Die Datenübertragung bei Online-Meetings findet stets verschlüsselt statt. Hierbei kommt eine sehr sichere 256-bit-AES Verschlüsselung zum Einsatz. WebEx bietet darüber hinaus die Möglichkeit, Meetings Ende-zu-Ende-verschlüsselt durchzuführen, was jedoch zu Einschränkung des Funktionsumfanges führt. Folgende Funktionen sind bei nach Aktivierung der Ende-zu-Ende-Verschlüsselung nicht mehr möglich:

- Meetings in einem persönlichen Raum
- Beitreten vor dem Gastgeber
- In Lobby verschieben
- Videogerät-fähige Meetings (Aufzeichnung des Meetings ist möglich)
- Cisco Mobile WebexMeetings-Web-App
- Linux-Clients
- Netzwerkbasierte Aufzeichnung
- Speichern von Sitzungsdaten, Abschriften, Meetingprotokollen usw.
- Freigabe von Ferncomputern

Datenschutz

Als amerikanischer IT-Dienstleister treffen Cisco Webex dieselben Datenschutzbedenken wie seine beiden Vorgänger. Nach Außerkrafttreten des Privacy Shield Abkommens hat der Konzern das Vertragswerk um EU-Standardvertragsklauseln erweitert, auch ein Auftragsverarbeitungsvertrag ist Bestandteil der Vereinbarung. Die Berliner Datenschutzbehörde hat Cisco WebEx trotzdem mit einer roten Ampel und damit mangelnder DSGVO-Konformität bewertet, wieder ohne Rücksichtnahme auf die Möglichkeit technische Einstellungen zur Verbesserung des Datenschutzes vornehmen zu können. Derzeit besitzt das Unternehmen lediglich ein Rechenzentrum innerhalb der EU (in Amsterdam), alle weiteren befinden sich in den USA, China oder Australien. Eine Abwicklung des gesamten europäischen Datenverkehrs, bzw. die Verarbeitung personenbezogener Daten innerhalb der EU ist somit noch nicht vollständig möglich, jedoch wurden in dem Bericht die Anstrengungen diesbezüglich lobend erwähnt. Laut Unternehmensführung sollen weitere europäische Rechenzentren Mitte 2021 in Betrieb gehen und der Mangel damit zur Gänze behoben werden.

Nutzungsempfehlung

Betreffend Verschlüsselung verwendet Cisco WebEx gleiche Sicherheitsstandards wie Zoom und MS Teams, ein Zugriff auf Daten von außerhalb ist demnach praktisch unmöglich.

Weiters wurde das Vertragswerk um europäische Standardvertragsklauseln erweitert, auch ein Auftragsverarbeitungsvertrag ist vorhanden. Darüber hinaus besteht die Möglichkeit Meetings Ende-zu-Ende-verschlüsselt stattfinden zu lassen, allerdings nur in Verbindung mit zahlreichen Einschränkungen betreffend Funktionalität.

Derzeit befindet sich nur ein Serverzentrum des Unternehmens im Europäischen Wirtschaftsraum, ein Export von Daten in die Vereinigten Staaten ist damit unumgänglich.

Unter Verwendung der Ende-zu-Ende-Verschlüsselungsfunktion ist eine rechtmäßige Nutzung durchaus möglich, betreffend Aufbau der Plattform, Funktionalität, Bedienerfreundlichkeit und Stabilität wäre aber Zoom die weit bessere Alternative.

Big Blue Button

Big Blue Button (BBB) ist ein Audio-und Videokonferenztool des kanadischen Non-Profit-Unternehmens BigBlueButton Inc. mit Firmensitz in Ottawa, Ontario. Es handelt sich hierbei um ein sogenanntes Open-Source-Programm, der Quellcode der Software ist demnach frei verfügbar und öffentlich einzusehen. Eine Installation von Zusatzsoftware ist nicht notwendig, da BBB über den Webbrowser gestartet werden kann. Bis zu 100 Personen können an virtuellen Meetings teilnehmen. BigBlueButton selbst hat keine grafische Oberfläche zum Verwalten von Benutzer*innen oder Räumen, was die Installation eines Plugin (z.B. Greenlight) nötig macht. Neben Audio- und Videokonferenzen bietet BBB auch die Möglichkeit Umfragen durchzuführen, gemeinsam am Whiteboard zu arbeiten, Untergruppenräume zu eröffnen, den Bildschirm mit anderen zu teilen oder über die Chatfunktion Dateien an einzelne oder alle Teilnehmer*innen zu übermitteln. BBB ist im Vergleich zu anderen Tools jedoch nicht sofort nutzbar, sondern muss zuerst auf einem zur Verfügung stehenden oder angemieteten Server aufgesetzt werden. Darüber hinaus haben einige Anbieter*innen von Lern- und Website-Systemen, wie zum Beispiel NextCloud, Drupal, Moodle und WordPress, BBB bereits in ihr Produkt integriert, bzw. bieten eine Integrationsoption an.

Kriterien

Verschlüsselung

Die Datenübertragung von Client zu Server wird mit einer Transportverschlüsselung gesichert. Eine Ende-zu-Ende-Verschlüsselung von Meetings oder Webinaren ist mit Stand März 2021 noch nicht Teil des Funktionsumfanges von Big Blue Button.

Datenschutz

Die Datenverarbeitung erfolgt ausschließlich auf den selbst gewählten Servern. Um eine DSGVO-konforme Datenverarbeitung gewährleisten zu können, müssen die selbstgewählten Server ihren Standort innerhalb des Europäischen Wirtschaftsraum haben. Sollte ein IT-Dienstleister beauftragt werden BBB aufzusetzen, muss im Vorfeld mit diesem ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen werden.

Muster dafür finden sich unter anderem auf der WKO-Homepage.[22] Da BBB lediglich eine Transportverschlüsselungsfunktion besitzt, was den Weg zwischen Server und Client sichert, sind die Daten theoretisch serverseitig einsehbar Weiters empfiehlt es sich beim Aufsetzen des Programmes die Aufnahmefunktion von vornherein manuell zu deaktivieren, ansonsten zeichnet BBB alle Videochats automatisch auf, auch wenn der Aufnahmeknopf nicht aktiv betätigt wurde. Die Videos sind dann bis zu zwei Wochen am Server gespeichert, was dem Grundsatz der Datenminimierung widersprechen würde. Sollte BBB als Videokonferenztool für den Unterricht verwendet werden, ist das Einholen einer Einverständniserklärung im Vorfeld unbedingt nötig[23].

[22] https://www.wko.at/branchen/handel/D_06a-Auftragsverarbeitungsvertrag-nach-Art-28-DSGVO.pdf
[23] Vorlage Einverständniserklärung: https://datenschutz-schule.info/2020/05/06/einwilligung-vorlagen-fuer-bigbluebutton/

Nutzungsempfehlung

Unter Einhaltung der technischen Datenschutzmöglichkeiten, ist eine DSGVO-konforme Verendung von BBB auf jeden Fall gegeben, besonders dann, wenn eigene Server zur Verfügung stehen und die Verarbeitung personenbezogener Daten sozusagen unter eigenem Dach stattfindet. Big Blue Button ist bezüglich Nutzeroberfläche, Bedienungsfreundlichkeit, Funktionsumfang, Stabilität und Zuverlässigkeit auf einem sehr guten Weg, jedoch noch nicht vergleichbar mit den großen Anbietern. Für kleinere betriebsinterne Meetings und Besprechung ist BBB eine absolut empfehlenswerte datensparende, rechtlich einwandfreie Alternative. Für große Veranstaltungen oder Konferenzen fehlt es jedoch noch an Performance.

Jitsi Meet

Jitsi ist ein Open Source Projekt, das 2003 an der Universität Straßburg initiiert wurde und mittlerweile zu einer Sammlung frei zugänglicher Software, unter anderem auch für Videokonferenzen (Jitsi Meet) angewachsen ist. Die Verwendung ist ohne Registrierung über den Browser möglich. Zum Funktionsumfang gehören HD-Videokonferenzen mit Audiofreigabe, Audio-Only-Konferenzen, Bildschirmfreigabe und Aufzeichnungsfunktion. Voraussetzung für die Nutzung ist ein dazugehöriger Server, über den die Verbindungen laufen.

Kriterien

Verschlüsselung

Alle Kommunikationswege, also Audio, Video und Chat bei Jitsi Meet sind mit einer Transportverschlüsselung gesichert. Darüber hinaus bietet die Plattform seit kurzem auch eine Ende-zu-Ende-Verschlüsselung von Videokonferenzen an.

Datenschutz

Bei Jitsi Meet werden weder Daten erzeugt noch länger als nötig verarbeitet. Der Zugang passiert über einen Browser, diesbezüglich fallen weder Konto- noch Zugangsdaten an. Alle Daten die nötig sind, um Meetings reibungslos stattfinden zu lassen, werden augenblicklich nach Beendigung der Veranstaltung wieder gelöscht. Zur datenschutzkonformen Durchführung von Videokonferenzen ist überdies die Auswahl eines Servers mit Standort innerhalb des Europäischen Wirtschaftsraumes vonnöten, der im besten Fall selbst betrieben bzw. nach Abschluss eines Auftragsverarbeitungsvertrages mit einem Hostingdienst angemietet werden sollte[24].

Nutzungsempfehlung

Jitsi Meet ist eine Videokonferenzplattform, die ebenso wie Big Blue Button aus der Intention heraus entwickelt wurde, eine datensparende, europäische Alternative zu amerikanischen Produkten auf Basis geltender Datenschutzgesetze auf den Markt zu bringen. Aufholbedarf besteht auf jeden Fall noch in puncto Leistung und Stabilität. Für kleinere Meetings, Teambesprechung oder Austausch online ist Jitsi Meet aber sicherlich empfehlenswert.

[24] Einer dieser Dienste die Videokonferenzen auf Jitsi-Basis mit Servern in Deutschland, Finnland und Österreich anbieten, ist fairmeeting (www.fairkom.eu)

Fazit

Außergewöhnliche Zeiten erfordern außergewöhnliche Maßnahmen. Gerade während der Coronazeit sollte der Fokus auf die effiziente Durchführung von Arbeitsprozessen liegen, leichte Bedienbarkeit, Leistungsfähigkeit und Stabilität der Anwendung sind unabdingbare Faktoren, die dafür nötig sind. Mit den entsprechenden organisatorischen Maßnahmen und technischen Adaptionen[25] steht der Verwendung führender Videokonferenzsysteme amerikanischer Unternehmen nichts im Wege. Nichtsdestotrotz sind auch die US-IT-Dienstleister gefordert vertraglich nachzubessern und die rechtlichen Rahmenbedingungen lückenlos an die Anforderungen der DSGVO anzupassen.
Betriebsintern ist eine Verwendung europäischer, datensparender, lückenlos DSGVO-konformer Alternativen[26] zu amerikanischen Anbietern für kleine Meetings, Besprechungen oder die Koordination von Arbeitsabläufen auf jeden Fall wünschens- und empfehlenswert.

[25] Allgemeine Voraussetzungen für Zulässige Nutzung von Zoom des BMBWF: https://www.bmbwf.gv.at/Ministerium/Datenschutz/Zoom.html
[26] Besonders BigBlueButton und Jitsi Meet

Anhang

Zoom

Datenschutzerklärung

- https://zoom.us/de-de/privacy.html
- https://www.blink.it/blog/wie-sicher-ist-zoom
- https://www.saferinternet.at/news-detail/zoom-oder-nicht-zoom/
- https://www.hu-berlin.de/de/pr/coronavirus-informationen/corona/videokonferenzen-mit-zoom
- https://video.cls.rwth-aachen.de/videoconferencing-in-der-le,hre/
- https://www.datenschutz-guru.de/zoom-ist-keine-datenschleuder/

MS Teams

Datenschutzerklärung

- https://privacy.microsoft.com/de-de/privacystatement
- https://docs.microsoft.com/de-de/compliance/regulatory/offering-eu-model-clauses

Cisco Webex

Datenschutzerklärung

https://www.cisco.com/c/de_de/about/legal/privacy-full.html

Standardvertragsklausel

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/mdpa-for-supplier-portal.pdf

Big Blue Button

Datenschutzerklärung

https://bigbluebutton.org/privacy/

Muster Auftragsverarbeitungsvertrag WKO

https://www.wko.at/branchen/handel/D_06a-Auftragsverarbeitungsvertrag-nach-Art-28-DSGVO.pdf

Vorlage Einwilligungserklärung Big Blue Button für den Unterricht

https://datenschutz-schule.info/2020/05/06/einwilligung-vorlagen-fuer-bigbluebutton/

Jitsi Meet

Datenschutzerklärung

https://jitsi.org/security/