Datenschutz Checkliste: Digitale Tools

Stand: 16. März 2021 (mit redaktionellen Änderungen vom 17.10.2022)

Aufgrund der derzeitigen Corona-Lage ist es für viele Jugendgruppen nicht ohne Weiteres möglich, die Jugenddienste in gewohnter Weise durchzuführen. In vielen Jugendgruppen gibt es daher schon länger digitale Jugenddienste oder sind gerade in der Planung. Zur Umsetzung gibt es eine Vielzahl von Möglichkeiten. So können z.B. neben einer Videokonferenz auch verschiedene Anwendungen genutzt werden, über die man sich austauschen, gemeinsam Ideen entwickeln, rätseln oder spielen kann. Dabei spielt das Thema Datenschutz eine immer wichtigere Rolle. Leider ist es nicht möglich, alle Apps, Websites oder sonstige Tools aufzulisten und ausreichend zu bewerten. Daher soll diese Checkliste euch dabei helfen, digitale Methoden hinsichtlich des Datenschutzes zu prüfen und euch bei der Auswahl der richtigen Tools zu unterstützen.

1. Was ist eigentlich Datenschutz und warum sollte ich bei der Jugendarbeit auf den Datenschutz achten?

Datenschutz bedeutet, dass man Daten anderer Personen nicht einfach so benutzen darf. Das sind z.B. Name, Geburtsdatum oder Emailadresse, sogenannte persönliche oder personenbezogene Daten. Jeder soll selber bestimmen können, wer etwas über ihn weiß. Die Regeln dafür sind in Gesetzen festgelegt, an die man sich auch in der Jugendarbeit halten muss. Besonders, weil man hier häufig mit den Daten von Jugendlichen und Kindern arbeitet, für die man verantwortlich ist. Das Datenschutzrecht ist in Deutschland durch mehrere Gesetze geregelt: der EU-Datenschutzgrundverordnung (EU-DSGVO), dem Bundesdatenschutzgesetz (BDSG) oder dem Telekommunikationsgesetz (TKG). Die wichtigsten Regelungen zum Schutz von persönlichen Daten finden sich in der EU-DSGVO. Diese gilt in allen Mitgliedsstaaten der EU und schreibt vor wie, z.B. Unternehmen mit einem Sitz in der EU oder Vereine mit den Daten von Kund:innen oder Mitgliedern umgehen dürfen. Bei der Nutzung von digitalen Anwendungen und Tools müssen diese Regeln also auch durch die Jugendgruppen und die Jugendbetreuer:innen berücksichtigt werden. Viele der Anwendungen, die man für einen digitalen Jugenddienst nutzen kann, kennt man zwar schon aus der Schule oder der Arbeit, trotzdem sollte jedes mal vor und während des Einsatzes darauf geachtet werden, dass korrekt und verantwortungsvoll mit den Daten anderer umgegangen wird.

2. Wie kann ich selber Software, Websites oder Apps überprüfen?

- Schaut auf der Website (z.B. Impressum) nach, wo der Sitz des:der Anbieter:in ist: Wenn eine Adresse in der EU genannt wird, ist dies ein gutes Zeichen, da sich der:die Anbieter:in dann an die Regeln der EU-DSGVO halten muss. Ein Sitz in Deutschland wäre die beste Möglichkeit. Liegt der Sitz z.B. in den USA wird es wahrscheinlicher, dass bestimmte Datenschutzstandards nicht eingehalten werden. Zusätzlich kann man über Seiten, wie z.B. www.utrace.de, prüfen, wo der:die Anbieter:in wirklich sitzt.

- Prüft, in welcher Sprache die Website verfasst ist. Eine deutschsprachige Website/Anwendung ist ein Hinweis darauf, dass der:die Anbieter:in sich im Zweifel an die EU-DSGVO hält.

- Prüft die Datenschutzerklärung (engl. Privacy Terms) des:der Anbieter:in:

  - Eine Datenschutzerklärung oder Datenschutzbestimmung ist eine Beschreibung, wie Daten (insbesondere personenbezogene Daten) von dem:der Anbieter:in verarbeitet werden. Hier sollte stehen, wie diese Daten gesammelt, genutzt oder ob sie an Dritte weitergegeben werden. Manchmal beschreibt der:die Anbieter:in auch, welche Maßnahmen ergriffen werden, um die Privatsphäre der Nutzer:innen zu wahren.

  - Prüft, ob sich die Datenschutzerklärung auf die EU-DSGVO bezieht. In englischen Texten könnt ihr z.B. nach „GDPR“ (General Data Protection Regulation) suchen, das ist die englische Bezeichnung für die EU-DSGVO. Eine Erklärung des:der Anbieter:in , dass man sich an die Regeln hält, ist oft schon ein guter erster Hinweis.

  - Wird klar, welche personenbezogenen Daten erhoben werden? Das können sein: Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usw. oder aber auch Onlinedaten wie IP-Adresse oder Standort. Macht der:die Anbieter:in hierzu gar keine Angaben, sollte eine Nutzung nochmal überdacht werden.

  - Werden erhobene personenbezogene Daten an Dritte, z.B. für Werbezwecke, übermittelt? Hier gilt, dass es besser ist, je weniger Daten weitergeleitet werden.

  - Übermittelt der:die Anbieter:in Daten an Drittstaaten? Am besten gibt es gar keine Übermittlung.

  - Nennt der:die Anbieter:in eine:n Ansprechpartner:in für die Betroffenenrechte? Also eine Stelle, an die man sich wenden kann, wenn man Auskunft über die bei der Nutzung erhobenen Daten erhalten möchte? So kann im Fall der Fälle eine Löschung der erhobenen Daten angestrebt werden.

  - Wie aktuell ist die Datenschutzerklärung? Durch ein Gerichtsurteil des Europäischen Gerichtshofs (EUGH) ist eine Abmachung zum Datenschutz zwischen der EU und den USA, der sog. „EU-US-Privacy Shield“ seit 16. Juli 2020 nicht mehr gültig. Alle Erklärungen, die älter als dieser Stichtag sind, sind nicht mehr ohne Weiteres gültig.

- Ist die Anwendung kostenlos nutzbar? Dies ist ein guter Hinweis darauf, dass eher mehr Daten der Nutzer:innen erhoben werden. Denn wenn eine Anwendung nicht mit Geld bezahlt wird, bezahlt man fast immer mit seinen Daten.

3. Was sollte ich beim Einsatz von digitalen Methoden beachten?

- Informiert die Junghelfer:innen und die Sorgeberechtigten darüber, dass ihr digitale Jugenddienste oder Maßnahmen plant und dass dabei ggf. persönlichen Daten erhoben werden können. Besonders wenn es Junghelfer:innen in der Gruppe gibt, die jünger als 16 Jahre

sind. Hier sollten die Sorgeberechtigten in jedem Fall informiert werden. Nutzt dafür am besten eine E-Mail oder einen Brief an alle Sorgeberechtigten.

- Falls für den digitalen Jugenddienst Daten der Junghelfer:innen, wie z.B. die Emailadressen, benötigt werden, sollte darüber ebenfalls im Vorfeld informiert werden. Am besten mit einer kurzen Begründung.

- Nennt in der Vorabinformation die Daten, die erhoben werden. Diese könnt ihr in den Datenschutzerklärungen des:der Anbieter:in finden.

- Nennt die digitalen Tools, die ihr benutzten wollt und stellt einen Link der Homepage und der Datenschutzerklärung des:der Anbieter:in zur Verfügung. So kann sich jede:r Betroffene:r selbst ein Bild machen.

- Achtet bei Videokonferenzen darauf, dass der Zugang passwortgeschützt ist und die Teilnehmenden sich so in einem geschützten Umfeld bewegen.

- Ihr solltet auf die Aufzeichnung von Videokonferenzen verzichten. Ist eine Aufzeichnung aber nötig, müsst ihr die Teilnehmenden vorher darüber informieren und um ihr Einverständnis bitten.

- Anwendungen, die ohne Anmeldung, das heißt z.B. ohne die Angabe einer Emailadresse für die Teilnehmenden zugänglich sind, erheben weniger Daten als solche, in denen zuerst ein komplettes Profil erstellt werden muss.

- Grundsätzlich gilt: plant so, dass so wenig Daten wie möglich nötig sind und fragt euch immer, ob die geforderten Daten für die Nutzung des Tools unbedingt notwendig sind.

- Dienste, die ihr selbst betreibt, sind am sichersten. Dies ist z.B. bei Videokonferenzlösungen möglich. Dazu ist aber nicht jede Ortsjugend in der Lage.

Hinweis: Diese Checkliste ist eine Handlungsempfehlung ohne Gewähr. Trotz sorgfältiger inhaltlicher Kontrolle übernimmt die THW-Jugend e.V. keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der Empfehlungen.