

WLAN in der Jugendhilfe:

Internetzugang und Haftungsfragen



Ein Überblick für Fachkräfte der Kinder- und Jugendhilfe

Autorin:

Britta Schülke (Juristin / Fachreferentin Recht / AJS NRW)

Aktualisierung:

Antje Lehbrink (AJS NRW)

Jelena Wachowski (AJS NRW)

Unter Mitarbeit von:

Susanne Philipp (AJS NRW)

Matthias Felling (AJS NRW)

Alexander Hundeborn (Projekt PowerUp / fjm NRW)

Stand: 10. August 2021

Das Internet ist fester Bestandteil im Alltag von Kindern und Jugendlichen. Dieser Entwicklung können und sollten sich auch Jugendhilfeeinrichtungen nicht verschließen. Bei den Überlegungen, ob ein Internetzugang „angeschafft“ werden soll, wird oft thematisiert, inwieweit Jugendlichen ein Internetzugang überhaupt „rechtssicher“ zur Verfügung gestellt werden kann – sei es mit dem PC vor Ort oder durch WLAN, welches Kinder und Jugendliche dann mit eigenen Smartphones oder Tablets nutzen können.

Inwieweit ist es möglich, einen offenen Internetzugang bereitzustellen, ohne dass für die Betreiber*innen des WLANs, also z. B. Jugendeinrichtungen oder Wohngruppen, die Gefahr besteht, selbst etwa wegen unerlaubter Downloads bzw. unerlaubtem Filesharing eines Dritten zur Verantwortung gezogen werden zu können? Zwar ist allseits bekannt, dass der Gesetzgeber im Oktober 2017 die sogenannte Störerhaftung abgeschafft hat, aber was bedeutet das konkret für die Praxis?

Was änderte der Wegfall der Störerhaftung?

Seit der Abschaffung der Störerhaftung am 13. Oktober 2017 ist das Haftungsrisiko für Anschlussinhaber*innen überschaubar geworden. Zuvor konnte mit Abstufungen grundsätzlich jede Person als Störer*in in Anspruch genommen werden, die einen Internetzugang bereithielt. Haftungsrisiken wegen kostspieliger Urheberrechtsverletzungen z. B. durch illegale Downloads von Musikvideos kamen rasch zustande.

Denn allein aufgrund des Vorhaltens des Internetzugangs bestand rechtlich eine potenzielle Ursächlichkeit bzw. Verantwortlichkeit bzgl. der Verbreitung rechtswidriger Inhalte oder illegalen Filesharings unabhängig von der tatsächlich eigenhändigen Veranlassung. Dieser Haftungsfall konnte WLAN-Anbieter*innen kaum rechtlich zuverlässig begegnen. Denn bis heute gibt es keine zumutbaren, umsetzungsfähigen technischen und tatsächlichen Möglichkeiten, den Missbrauch durch fremde Nutzer*innen in Gänze zu verhindern.

Da sich diese rechtliche Unsicherheit nachteilig auf die Verbreitung freier WLAN-Zugänge auswirkte, schaffte der Gesetzgeber unter Berücksichtigung der EU-Vorgaben die Störerhaftung ab. Im Gegenzug können Rechteinhaber*innen nun Netzsperrungen verlangen, sofern sie verhältnismäßig und zumutbar sind (§ 7 Abs. 4 TMG).

§ 8 Telemediengesetz (TMG) Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

(3) Die Absätze 1 und 2 gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

(4) Diensteanbieter nach § 8 Absatz 3 dürfen von einer Behörde nicht verpflichtet werden,

1. vor Gewährung des Zugangs
 - a) die persönlichen Daten von Nutzern zu erheben und zu speichern (Registrierung) oder
 - b) die Eingabe eines Passworts zu verlangen oder
2. das Anbieten des Dienstes dauerhaft einzustellen.

Davon unberührt bleibt, wenn ein Diensteanbieter auf freiwilliger Basis die Nutzer identifiziert, eine Passwordeingabe verlangt oder andere freiwillige Maßnahmen ergreift.

Personen, die einen Internetanschluss öffentlich zur Verfügung stellen, haften seit der Abschaffung der Störerhaftung **grundsätzlich nicht** mehr für das rechtswidrige Verhalten von Nutzer*innen.

Für das Greifen dieser Haftungsprivilegierung ist es gemäß § 8 Abs. 4 TMG unerheblich, ob das WLAN-Angebot frei zugänglich oder passwortgebunden ist und/oder eine Registrierung seiner Nutzer*innen verlangt.

Gilt die Haftungsprivilegierung auch privat?

Von dieser Haftungserleichterung profitieren nicht nur öffentliche WLAN-Anbieter*innen wie Café-, Hotel- und andere Hotspotbetreiber*innen sowie Einzelhändler*innen, Touristeninformationen, Bürgerämter oder Krankenhäuser. **Sie gilt auch für private WLAN-Betreiber*innen im Rahmen ihres Internetanschlusses.**¹ Dies widerspricht auch nicht dem Vollharmonisierungsgrundsatz der EU-Richtlinie, die Grundlage für die Abschaffung der Störerhaftung gewesen ist und eine entsprechende Haftungsprivilegierung für kommerzielle Anbieter vorsieht, da die EU keine Regelung für den „privaten Bereich“ vorgibt.²

Für Einrichtungen der Kinder- und Jugendhilfe, unabhängig von ihrem Charakter als Wohngemeinschaft oder offenem Angebot, bedeutet dies, dass sie risikofrei Kindern und Jugendlichen WLAN zur Verfügung stellen können.³

Gibt es eine verbindliche Altersgrenze?

Für den Zugang zum Netz gibt es keine verbindliche gesetzliche Altersgrenze. Die von der DSGVO vorausgesetzte Vollendung des 16. Lebensjahrs betrifft nur die Verarbeitung von personenbezogenen Daten bei Angeboten von „Dienstleistungen der Informationsgesellschaft“ und dürfte daher keine Auswirkungen haben. Die Regelungswerke zielen auf ganz unterschiedliche Schutzgüter ab.

Bei der Altersgrenze der DSGVO geht es darum, Kinder und Jugendliche vor möglichen Datenmissbrauchsrisiken zu schützen. Die Haftungsprivilegierung bzw. der Wegfall der Störerhaftung des § 8 TMG verfolgt dagegen die Intention, dass WLAN-Anbieter*innen nicht für Rechtsverstöße zur Verantwortung gezogen werden sollen, die sie selbst nicht

¹ Spindler / Schmitz, TMG-Kommentar, 2. Auflage, § 8 Rn. 26

² Ebenda; ders. Mantz / Sassenberg, MMR 2015, 85, 87;

Nordemann, GRUR 2016, 1097, 1098f.

³ Das OLG München (Urt. v. 15. März 2018 – 6 U 1741/17) hat die

begangen haben bzw. von denen sie selbst nichts wussten.

Welche technischen Möglichkeiten gibt es?

Wer trotz der geänderten Rechtslage mit der Haftungsprivilegierung nicht selbst als WLAN-Anbieter*in auftreten möchte, kann einen externen Dienstleistenden für **WLAN-Hotspots** gegen Entgelt beauftragen. Besonders in der Hotelbranche ist diese Lösung seit Jahren verbreitet. Dies liegt zum einen an der einfacheren Verwaltung und zum anderen auch an der kompletten Haftungsauslagerung, was sicherlich besonders auf die alte Rechtslage zurückzuführen ist. Preislich fangen solche Lösungen bei ca. 15 Euro im Monat an. Verschiedene Anbieter*innen lassen sich schnell im Internet recherchieren.

Was sagt die Medienpädagogik?

Die Haftungsprivilegierung führt dazu, dass Kinder und Jugendliche aus rechtlicher Sicht grundsätzlich nicht mehr beim „Surfen“ beobachtet oder über Gebühr überwacht werden müssen. Auch gibt es keine gesetzlich festgelegten Altersgrenzen für die Nutzung des Internets.

Für die Medienpädagogik bedeutet das, dass ihre **Ansätze zur Vermittlung von Medienkompetenz wichtiger denn je sind**. Aus medienpädagogischer Sicht sollten Kinder und Jugendliche dazu befähigt werden, mit den unbegrenzten Inhalten und Möglichkeiten im Netz verantwortungsvoll umzugehen. Deshalb sollte in der Einrichtung im Zusammenhang mit der Bereitstellung von Internetzugängen Folgendes geklärt werden:

- ✓ Festlegen von Altersregelungen für den Zugang zum Internet (jüngere Kinder sind sicher aufsichtsbedürftiger als Jugendliche)
- ✓ Verhaltensregeln
- ✓ Kommunikationsregeln für Soziale Netzwerke (Netiquette, Hate Speech, Mobbing)
- ✓ Achtsamkeit bei der Eingabe von Daten
- ✓ Sensibilisierungsansätze der DSGVO
- ✓ Umgang mit „Fake News“
- ✓ Ansprechpartner*innen für Problemfälle (Vertrauensperson benennen – an wen können sich Kinder und Jugendliche wenden, wenn sie Sorgen haben oder auf verstörende Inhalte stoßen)

!! Praxistipp !!

WLAN-Nutzungsbedingungen

Medienpädagogische Ansätze können recht gut anhand von WLAN-Nutzungsbedingungen vermittelt und diskutiert werden. So bietet es sich an, die Regeln gemeinsam mit den Kindern und Jugendlichen auszuhandeln. Der Zugang zum WLAN sollte dann an die Akzeptanz dieser Nutzungsbedingungen gekoppelt werden. Technisch lassen sich solche Voraussetzungen gut umsetzen.



DSGVO beachten

- 16 Jahre als Altersgrenze für Einwilligungen bei Datenverarbeitungsvorgängen, sonst Einwilligung der Sorgeberechtigten erforderlich
- Information und Transparenz über etwaige damit zusammenhängender Datenverarbeitungsvorgänge in verständlicher Sprache (z. B.: Werden temporär die besuchten Seiten gespeichert?)

Was gilt für LAN-Verbindungen?

Im Jahr 2018 entschied der Bundesgerichtshof, dass die Einschränkungen der Störerhaftung, die mit der Änderung der Haftungsprivilegierung in Kraft getreten sind, auch für die Zugangsvermittler von drahtgebundenen Anschlüssen gelten.⁴ Für Einrichtungen, die ihren Bewohner*innen den Zugang zum Netz mittels LAN-Anschluss an das eigene Endgerät ermöglichen, dürften daher grundsätzlich keine Haftungsverteile oder -nachteile im Verhältnis zur Zugangsvermittlung mittels WLAN geltend gemacht werden können.

Wer muss was beweisen?

Kommt es – z. B., weil ein Musikstück illegal über einen Anschluss heruntergeladen wurde – zu einem Gerichtsverfahren, stellt sich die Frage wer darzulegen und zu beweisen hat, auf welche Person dieser illegale Download zurückzuführen ist. Ganz grundsätzlich trifft diese Darlegungs- und Beweislast den oder die Inhaber*in des Urheberrechts – wie z. B. die Gesellschaft, die die Rechte an dem Musikstück erworben hat. Handelt es sich um einen WLAN-Anschluss,

⁴ BGH ZUM 2018, 705 (709f) – Dead Island

der von einer Einzelperson angeboten wird, gilt allerdings die gesetzliche Vermutung, dass der oder die Anschlussinhaber*in selbst die Rechtsverletzung begangen hat.⁵

Keine Panik: Dieser Vermutung können WLAN-Anschlussinhaber*innen durch die Darlegung, dass zu dem fraglichen Zeitpunkt auch andere Personen den Anschluss nutzten,⁶ in den allermeisten Fällen effektiv entgegenzutreten. Die Identitäten der Nutzenden müssen nämlich nur vorgetragen oder erforscht werden, wenn dies den Anschlussinhaber*innen im Einzelfall zuzumuten ist. An die Zumutbarkeit der Identitätspreisgabe stellt der Bundesgerichtshof zu Recht hohe Anforderungen. So entschied er beispielsweise im Jahr 2016, dass von Ehepartner*innen nicht verlangt werden könne, das Nutzungsverhalten des oder der Partner*in zu dokumentieren oder dessen bzw. deren Computer zu durchsuchen.⁷

Für die Frage, ob die Preisgabe von Identitäten von Nutzer*innen im Betätigungsfeld der Kinder- und Jugendhilfe zumutbar ist, verdient zudem das allgemeine Persönlichkeitsrecht noch einmal einen ganz besonderen Schutz. Es bildet die Grundlage des Vertrauens zu den Fachkräften, das für die Wirksamkeit pädagogischer Maßnahmen unabdingbar ist. Spätestens dort, wo die Grenzen des Sozialdatenschutzes überschritten werden, findet die Zumutbarkeit von Nachforschungspflichten und Kontrollen daher ihr Ende.

Wie genüge ich der Aufsichtspflicht?

Wenn die Rechtsverstöße den Anschlussinhaber*innen nicht bewiesen werden können – was immer dann der Fall sein dürfte, wenn mehrere Zutritt zu dem Rechner haben (klassischer Fall in der Einrichtung) – kann aber noch eine Haftung des für die Kinder und Jugendlichen zuständigen Aufsichtspflichtigen nach § 832 BGB in Betracht kommen.

Einrichtungen, die Kinder und Jugendliche über eigene Computer die Nutzung des Internets ermöglichen wollen, sollten, um die Belehrungspflichten zu erfüllen, Nutzungsvereinbarungen mit den Kindern und Jugendlichen abschließen.

Die Rechtsprechung verlangt in diesem Zusammenhang relativ wenige Maßnahmen treffen und fordert insbesondere keine ständige Überwachung der Kinder oder ihrer Endgeräte. Die „einfache **Belehrung**,

keine Rechtsverletzungen zu begehen, reicht aus.⁸ Eine Verpflichtung, die Nutzung des Internets durch ein Kind zu überwachen, den Computer des Kindes zu überprüfen oder dem Kind den Zugang zum Internet (teilweise) zu versperren, besteht grundsätzlich nicht. Derartige Maßnahmen werden – so der BGH – erst zur Pflicht, wenn konkrete Anhaltspunkte für eine rechtsverletzende Nutzung des Internetanschlusses durch das Kind bestehen.

Geht es um den Internetanschluss der Eltern, verlangt der BGH auch nicht, dass die vorzunehmenden Belehrungen der Kinder dokumentiert werden müssen.

!! Praxistipp !!

Nutzungsvereinbarungen

Einrichtungen, die Kindern und Jugendlichen über eigene Computer die Nutzung des Internets ermöglichen wollen, sollten, um die Belehrungspflichten zu erfüllen, Nutzungsvereinbarungen mit den Kindern und Jugendlichen abschließen. Dies ermöglicht auch hervorragend die Implementierung medienpädagogischer Ansätze zur Vermittlung von Medienkompetenz.

Der Zugang zum Internet sollte abhängig von der Akzeptanz der Nutzungsvereinbarungen gemacht werden. Hier ist sowohl das eigenhändige Unterschreiben der Vereinbarungen durch die Jugendlichen als auch die Belehrung in Form der Anklick-Option auf dem Computer denkbar. Das eigenhändige Unterschreiben dürfte von Kindern und Jugendlichen wohl als verbindlicher empfunden werden und bietet zudem den Vorteil der nachweisbaren Dokumentation.



DSGVO beachten

- 16 Jahre als Altersgrenze für Einwilligungen bei Datenverarbeitungsvorgängen, sonst Einwilligung der Sorgeberechtigten erforderlich
- Information und Transparenz über etwaige damit zusammenhängender Datenverarbeitungsvorgänge in verständlicher Sprache (z. B.: Werden temporär die besuchten Seiten gespeichert?)

⁵ Knies, Zur sekundären Darlegungslast und tatsächlichen Vermutung in Filesharing-Prozessen, www.new-media-law.net, Abrufdatum: 7. Februar 2021, m. w. N.

⁶ BGH NJW 2014, 2360 - Bearshare

⁷ BGH GRUR 2017, 386 - Afterlife

⁸ BGH GRUR 2013, 511 - Morpheus

!! Praxistipp !!

Technische Umsetzung von WLAN

Kommerzielle Anbieter*innen (z. B. The Cloud, Lan1) bieten neben Infrastruktur auch administrative Umsetzungen und Wartung an.

Vorteile: Haftungsfrage geklärt / Jugendschutzfilter möglich / datenschutzsicher / pädagogische Umsetzung über Verstärkerpläne möglich

Nachteile: Kosten (sowohl monatlich als auch für die einmalige Anschaffung) / wenig eigene Gestaltungsmöglichkeiten

Bei einem **hausinternen Aufbau eines WLAN**, bei dem auch **nicht-kommerzielle Anbieter** genutzt werden (z. B. durch Nutzung von Freifunk oder die Einrichtung von Gast-Zugängen am Router), wachsen die Gestaltungsmöglichkeiten.

Vorteile: wenig kostenintensiv / freier Zugang zum Internet / bei Freifunk auch die Haftungsfrage geklärt / pädagogischer Umgang viel stärker im Diskurs (Kompetenzen der Nutzenden gefordert)

Nachteile: keine Jugendschutzfilter routerseitig möglich / Wartung muss selbst oder auf Anfrage bei gemeinnützigen Vereinen geleistet werden / bei Gast-Zugang Gefahr der Haftung bzw. Unterlassungserklärungen

www.internet-abc.de/kinder/lernen-schule/surfschein/

Mit dem Surfschein lernen Heranwachsende spielerisch, welche Regeln im Netz zu beachten sind.

!! Praxistipp !!

Alternative Messenger

Es gibt Messenger, die ähnliche Funktionen bieten wie der Marktführer WhatsApp und trotzdem über höhere Datenschutzstandards verfügen. Hierzu zählen zum Beispiel Signal (allerdings mit Serverstandort in den USA) und Threema (Server in der Schweiz). Weitere, weniger bekannte Dienste mit hohem Datenschutzstandard sind...

wire: Server in Deutschland und Irland/ private Anwendung kostenlos / für iOS und Android verfügbar

ginlo: Hervorgegangen aus SIMSMe / Server in Deutschland / für iOS und Android verfügbar

Link-Tipps

<https://irights.info/artikel/privates-offentliches-und-gewerbliches-wlan-wer-haftet-wann/17925>

Die Fachleute von irights.info geben einen Überblick zum Thema Haftungsfragen und verlinken auch WLAN-Nutzungsvereinbarungen.

www.klicksafe.de/themen/schutzmassnahmen
Gute Übersicht zu Filtern und Jugendschutzprogrammen für Computer und mobile Geräte.

www.projekt-powerup.de/

Das Projekt „PowerUp | Medienpädagogik und Erziehungshilfe“ der Fachstelle für Jugendmedienkultur NRW hilft bei der Erstellung von Medienkonzepten. Auch hier findet sich eine Mustervereinbarung zur WLAN-Nutzung.

www.mediennutzungsvertrag.de/

Ein Baukasten hilft bei der Aufstellung eines Vertrags zur Mediennutzung. Ein Projekt von klicksafe und dem Internet ABC.