

WLAN in der Jugendhilfe: Internetzugang und Haf- tungsfragen



Ein Überblick für Fachkräfte der Kinder- und Jugendhilfe

Autorin:

Britta Schülke (Juristin / Fachreferentin Recht / AJS NRW)

Unter Mitarbeit von:

Susanne Philipp (AJS NRW)

Matthias Felling (AJS NRW)

Alexander Hundenborn (Projekt PowerUp / fjm NRW)

Stand: 03.07.2018

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 Smartphone oder Tablets nutzen können.

Inwieweit ist es möglich, einen offenen Internetzugang bereitzustellen, ohne dass für den Betreiber des WLANs, also z. B. die Jugendeinrichtung, die Gefahr besteht, selbst etwa wegen unerlaubten Downloads bzw. unerlaubten Filesharings 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?

Abschaffung der Störerhaftung

Seit der Abschaffung der Störerhaftung am 13.10.2017 ist das Haftungsrisiko für Anschlussinhaber überschaubar geworden. Zurvor konnte mit Abstufungen grundsätzlich jede/r als Störer/-in in Anspruch genommen werden, die/der einen Internetzugang bereithielt. Haftungsrisiken wegen kostspieliger Urheberrechtsverletzungen durch beispielsweise 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 Haftungsfalle konnten WLAN-Anbieter kaum rechtlich zuverlässig begegnen. Denn bis heute gibt es keine zumutbaren, umsetzungsfähigen technischen und tatsächlichen Möglichkeiten, den Missbrauch von (fremden) 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 Passworteingabe verlangt oder andere freiwillige Maßnahmen ergreift.

Haftungsprivilegierung – Unterscheidung nach Zugriffsmöglichkeit auf das Internet

Die Begrenzung des Haftungsrisikos – die sog. Haftungsprivilegierung – nach § 8 TMG greift zwar häufig, aber nicht immer. Haftungsrechtlich relevant ist dabei die Unterscheidung zwischen der Bereitstellung eines Endgerätes mit Internetzugang (klassischer Weise zum Beispiel der PC in der Jugendeinrichtung) und der Bereitstellung eines Internetzugangs via WLAN, der dann mit eigenem Smartphone, Tablet oder Laptop genutzt wird.

I. WLAN

WLAN-Anbieter sind diejenigen, die Dritten drahtlos über ein lokales Netzwerk den Zugang zum Internet ermöglichen. Sie haften gem. § 8 Abs. 3 TMG seit der Abschaffung der Störerhaftung **grundsätzlich nicht** für das rechtswidrige Verhalten ihrer Nutzer/-innen, da sie in der Regel nicht für das Verhalten ihrer Nutzer/-innen verantwortlich sein und es üblicherweise auch nicht kennen dürften.

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

Haftungsprivilegierung gilt auch privat

Von der Haftungserleichterung profitieren nicht nur öffentliche WLAN-Anbieter wie Café-, Hotel- und andere Hotspotbetreiber sowie Einzelhändler, Touristeninformationen, Bürgerämter oder Krankenhäuser. **Sie gilt auch für private WLAN-Betreiber 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 der Kinder- und Jugendhilfe, bedeutet dies, dass sie weitestgehend

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

² Ebenda; ders. Mantz / Sassenberg, MMR 2015, 85,87; Nordemann, GRUR 2016, 1097,1098f.

risikofrei, Kindern und Jugendlichen WLAN zur Verfügung stellen können. Zumal mit dem OLG München bereits das erste Gericht die Abschaffung der Störerhaftung für private WLAN-Anbieter bestätigt hat – vgl. OLG München, Urteil v. 15.03.2018 – 6 U 1741/17.

Altersgrenze von 16 Jahren nach DSGVO ändert nichts

Die nun von der DSGVO festgelegte Altersgrenze von 16 Jahren für ein gültiges Einverständnis von Kindern und Jugendlichen für die Verarbeitung von personenbezogenen Daten bei Angeboten von „Dienstleistungen der Informationsgesellschaft“ dürfte hierauf keine Auswirkungen haben. Der Zugang zum Internet unterliegt keiner abstrakten Altersgrenze. Zudem zielen die Regelwerke 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 nicht für Rechtsverstöße zur Verantwortung gezogen werden sollen, die sie selbst nicht begangen haben bzw. von denen sie selbst nichts wussten.

Externe Hotspotanbieter

Wer trotz der geänderten Rechtslage mit der Haftungsprivilegierung nicht selbst als WLAN-Anbieter auftreten möchte, kann einen externen Dienstleister 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 Haftungsübertragung, was sicherlich besonders auf die alte Rechtslage zurückzuführen ist. Preislich fangen solche Lösungen bei ca. 15 Euro im Monat an. Verschiedene Anbieter 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“ beaufsichtigt 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 sind 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 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.



Neuerungen der DSGVO beachten, Nutzungsbedingungen ggf. anpassen:

- 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?).

II. Nutzung des Internets über einen Computer der Einrichtungen oder über LAN-Verbindungen

Wird Kinder und Jugendlichen der Zugang zum Internet über einen Computer der Einrichtung selbst oder über eine Kabelverbindung (LAN) ermöglicht, kommt es nicht zum Wegfall der Störerhaftung bzw. zum Greifen der Haftungsprivilegierung. Dies liegt daran, dass der Kreis der potenziellen Nutzer hier überschaubarer ist und der Gesetzgeber dann Kontroll- und Prüfpflichten des Anschlussinhabers grundsätzlich für zumutbar hält.

Es besteht daher zunächst die gesetzliche Vermutungsregelung, dass die der IP-Adresse zugeordneten Rechtsverstöße vom Anschlussinhaber bzw. der Anschlussinhaberin begangen worden sind. Beweist er/sie, dass er/sie zum Zeitpunkt der Rechtsverletzung den Zugang nicht genutzt hat oder besteht die ernsthafte Möglichkeit, dass andere den Internetanschluss benutzt haben, gilt diese Vermutung als widerlegt. Hierfür muss der/die Anschlussinhaber/-in Tatsachen vortragen, dass andere Personen auch Zugang zum Internetanschluss hatten und diesen womöglich genutzt haben. Dann obliegt es den Anspruchsgegnern, das Gegenteil zu beweisen.

Haftungsrisiko durch „Belehrung“ begehen

Wenn die Rechtsverstöße den Anschlussinhabern 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 Jugendliche zuständigen Aufsichtspflichtigen nach § 832 BGB sowie die Störerhaftung in Betracht kommen.

Die Rechtsprechung verlangt in diesem Zusammenhang, dass Anschlussinhaber, die minderjährigen Kindern die Nutzung des Anschlusses ermöglichen, im Interesse der selbständigen Entwicklung der Kinder relativ wenige Maßnahmen treffen, insbesondere keine ständige Überwachung und keine komplette Überwachung des Computers der Kinder. Die „einfache“ Belehrung, keine Rechtsverletzungen zu begehen, reicht aus (Morpheus-Entscheidung des BGH, GRUR 2013, 511). Eine Verpflichtung, die Nutzung des Internet durch ein Kind zu überwachen, den Computer des Kindes zu überprüfen oder dem Kind den Zugang zum Internet (teilweise) zu versperren, besteht grundsätzlich nicht. Derartigen

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 Kinder und Jugendliche über eigene Computer die Nutzung des Internets ermöglichen wollen, sollten, um die Belehrungspflichten zu erfüllen, Nutzungsvereinbarungen mit den Kinder- und Jugendlichen abschließen. Dies ermöglicht auch hervorragend die Implementierung medienpädagogische Ansätze zur Vermittlung von Medienkompetenz hervorragend implementiert werden.

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.



Neuerungen der DSGVO beachten,
Nutzungsbedingungen ggf. anpassen:

- 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?).

IV. 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.

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

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

!! Praxistipp !!

Technische Umsetzung von WLAN

Kommerzielle Anbieter (z. B. TheCloud, 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

!! Praxistipp !!

Alternative Messenger

Es gibt Messenger, die ähnliche Funktionen bieten wie der Marktführer WhatsApp und trotzdem dem deutschen Datenschutz entsprechen.

Hier zwei Beispiele:

Hoccer: keine Handynummer zur Anmeldung notwendig / Server in Deutschland / kostenlos / keine Werbung / für iOS und Android verfügbar

SimsMe: Messenger der deutschen Post / in der privaten Variante kostenlos, aber werbefinanziert / Anmeldung via Handynummer notwendig / Funktionen näher an denen von WhatsApp / für iOS und Android verfügbar