Rechtliche Grundlagen

Ressourcen für den Umgang mit Fragen rund um Lizenzen, Datenschutz und andere Rechtsfragen
Der Prototype Fund bietet keine individuelle Rechtsberatung an. Bei den hier dargestellten Informationen handelt es sich lediglich um allgemeine Informationen.

- Lizenzierung und Urheberrecht
- Datenschutz
- Linksammlung Recht und rechtliche Angelegenheiten
- Überblick Markenrecht - StuFiS
- Verantwortung für Software und Inhalte

Lizenzierung und Urheberrecht

Software, deren Code veröffentlicht wird, ist grundsätzlich per Default, auch ohne Lizenz urheberrechtlich geschützt und darf nicht kopiert, verändert oder verbreitet werden (§ 69a u. § 69c UrhG) . Erst durch eine Open-Source-Lizenzierung werden anderen diese Rechte gewährt. Damit es sich bei einem neuen Projekt wirklich um Open-Source-Software handelt und andere von ihr profitieren sowie eigenständig an der Entwicklung mitwirken können, ist es deshalb wichtig, Code von Beginn an unter einer entsprechenden Lizenz zu veröffentlichen.

Lizenzen in der Entwicklung von Open-Source-Software

Lizenzen

Eine Softwarelizenz legt die Bedingungen fest, unter denen die Nutzung und Weitergabe der Software erlaubt bzw. verboten ist. Für Open-Source-Software existiert eine Vielzahl von Lizenzen. Sie alle haben gemeinsam, dass sie erlauben, den lizenzierten Quellcode unentgeltlich zu nutzen, zu teilen, zu ändern und weiterzuverbreiten. Unterschiede bestehen zwischen ihnen in Bezug darauf, unter welchen Bedingungen die Nutzung und Verbreitung des Codes erlaubt ist:

- **Permissive/Freizügige Lizenzen:** Für die Verbreitung von Kopien des Codes und darauf aufbauende Weiterentwicklungen dürfen Softwarelizenzen frei gewählt werden; selbst die Veröffentlichung unter proprietärer Lizenz ist erlaubt. Beispiele für diese Lizenzform sind MIT, BSD und Apache.
- **Copyleft-Lizenzen:** Die Verbreitung von Codekopien und von darauf aufbauenden Weiterentwicklungen ist erlaubt, muss aber unter derselben Lizenz erfolgen, unter der der Code ursprünglich veröffentlicht wurde. Unterschiede bestehen in Bezug darauf, wie weit die Veröffentlichungspflicht verstanden wird.
  - Schwaches Copyleft: Bei Lizenzen mit sogenanntem schwachen Copyleft ist es erlaubt, nur den veränderten Code unter derselben Lizenz zu veröffentlichen und diesen durch Verlinkung in proprietäre oder anders lizenzierte Software einzubinden. Beispiele sind die GNU Lesser General Public License (LGPL) und die Mozilla Public License (MPL).
  - Starkes Copyleft: Lizenzen mit starkem Copyleft erfordern die Veröffentlichung des gesamten Codes, in dem Codekopien bzw. Weiterentwicklungen genutzt werden. Ein Beispiel hierfür ist die GNU General Public License (GPL). Besonders weit geht die

GNU Affero General Public License (AGPL). Sie fordert auch dann die vollständige Veröffentlichung unter derselben Lizenz, wenn die ursprünglich unter AGPL lizenzierte Software bzw. eine darauf aufbauende Weiterentwicklung als Dienstleistung gehostet wird, ohne dass es zu einer Verbreitung des Codes selbst kommt (Software as a Service).

Lizenzauswahl

Welche Lizenz die richtige ist, hängt von einer Reihe von Faktoren ab. Dazu gehören z. B.:

- **Einfachheit und Bekanntheit:** Generell gilt, je einfacher und je bekannter eine Lizenz ist, desto leichter fällt es anderen zu verstehen, wie sie die Software nutzen und dazu beitragen können. Eine einfache und bekannte Lizenz kann so dazu beitragen, dass eine Community aus Nutzenden und Beitragenden um ein Open-Source-Projekt entsteht.
- **Beliebtheit in der Community:** Wenn ein Projekt an Open-Source-Software anknüpft, um die bereits eine aktive Community besteht, ergibt es oft Sinn, sich an der Lizenzierungspraxis dieser Community zu orientieren. Dahinter können Werte stehen, die in dieser Community als besonders wichtig erachtet werden und einen Einfluss darauf haben, ob Mitglieder sich an der Entwicklung eines neuen Projekts beteiligen. Zusätzlich kann die Verwendung derselben Lizenz eine Voraussetzung dafür sein, Weiterentwicklungen in bestehende Projekte integrieren.
- **Kompatibilität mit anderen Lizenzen:** Nicht alle Open-Source-Lizenzen sind miteinander kompatibel. Open-Source-Software mit inkompatiblen Lizenzen darf nicht kombiniert werden. Deshalb hat die Kompatibilität der gewählten Lizenz einen Einfluss auf die Verbreitung von Software. Copyleft-Lizenzen, die strengere Anforderungen enthalten, haben tendenziell eine geringere Kompatibilität.
- **Eignung für eine Kommerzialisierung:** Wenn aufbauend auf einem Open-Source-Projekt ein Geschäftsmodell entwickelt werden soll, spielen Wettbewerbsvorteile eine Rolle. Copyleft-Lizenzen untersagen beispielsweise, dass Wettbewerber den so veröffentlichten Code für Weiterentwicklungen in proprietärer Software nutzen. Unter permissiver Lizenz veröffentlichte Software hat dagegen unter Umständen bessere Chancen von Unternehmen genutzt zu werden, die Sorge davor haben, den eigenen Code veröffentlichen zu müssen.

Lizenzierung

Sobald die richtige Lizenz für ein Projekt gefunden wurde, ist das Lizenzieren einfach. Es genügt, im Repository, in dem der Code veröffentlicht ist, ein Dokument mit dem Namen LICENSE anzulegen und darin den Text der ausgewählten Lizenz zu kopieren bzw. aus einem im Repository verfügbaren Template auszuwählen.

Lizenzänderungen

Grundsätzlich ist es möglich, die Lizenz eines Open-Source-Projekts zu ändern. Voraussetzung dafür ist jedoch, dass alle Urheber der Änderung ausdrücklich zustimmen. Das sind in der Regel alle Personen, die zur Entwicklung der Software beigetragen haben. Wurde Code von Angestellten

geschrieben, kann das Nutzungsrecht daran allerdings auch bei deren Arbeitgeber*innen liegen (§ 69b UrhG). Alternativ zur Lizenzänderung kann für die Weiterentwicklung auch eine andere, mit der bisherigen kompatible Lizenz verwendet werden. Bei permissiven Lizenzen ist es außerdem möglich, eine Kopie des Projekts unter anderer Lizenz weiterzuentwickeln.

Lizenzverstöße

In Deutschland kann jede*r Urheber*in, der oder die an einem Open-Source-Projekt mitgewirkt hat, juristisch gegen Lizenzverstöße vorgehen (§ 8 Abs. 2, Satz 3 UrhG). Mögliche Konsequenzen eines Urheberrechtsverstoß reichen vom Unterlassungsanspruch gegen die Verbreitung der Software bis hin zu Schadensersatzansprüchen. Auch in Open-Source-Projekten selbst kann es zu Lizenzverstößen kommen, wenn Code beigetragen wird, der nicht unter der Lizenz des Projekts veröffentlicht werden darf. Insbesondere in Projekten, deren Software aktiv kommerziell oder auch nicht-kommerziell vertrieben wird, wird mit Beitragenden deshalb manchmal ein Contributor License Agreement (CLA) oder ein Developers Certificate of Origin (DCO) abgeschlossen, um Urheberrechtskonformität sicherzustellen.

Relevante Gesetze

Urheberrechtsgesetz (UrhG): Darin ist festgelegt, welche Rechte Personen haben, die als Urheber*innen Software entwickelt haben, wie sie diese durchsetzen können und welche Konsequenzen sich aus einem Urheberrechtsverstoß ergeben. Spezifische Regelungen für Software finden sich in §§ 69a ff. UrhG.

Wichtige Organisationen

ifrOSS, Institut für Rechtsfragen der Freien und Open Source Software: ifrOSS ist ein privates Institut, dessen Team zu rechtswissenschaftlichen Fragen rund um Open-Source-Software forscht, veröffentlicht und Vorträge hält. Ein Hauptfokus liegt dabei auf Open-Source-Lizenzen.

Open Source Initiative (OSI): Die US-amerikanische Organisation gibt eine breit akzeptierte Open-Source-Definition heraus und zertifiziert anhand dieser Definition Softwarelizenzen.

Weiterführende Links

- Einführung in den Schutz von Computerprogrammen, Universität Bremen: https://www.uni-bremen.de/urheberrecht/wissensplattform/8-schutz-von-computerprogrammen
- Überblick über verschiedene Open-Source-Lizenzen, GitHub: https://choosealicense.com/appendix/

- Von der Open Source Initiative zertifizierte Open-Source-Lizenzen, Open Source Initative: https://opensource.org/licenses
- Übersicht dazu, welche Lizenzen Projekte des Prototype Fund nutzen, Prototype Fund: https://prototypefund.de/projects/?filter=dataviz
- FAQ zu Lizenzierungsfragen in Open-Source-Projekten, GitHub: https://opensource.guide/legal/
- Vortrag zu Open-Source-Lizenzen und -Geschäftsmodellen, Frank Karlitschek (Nextcloud): https://archive.fosdem.org/2020/schedule/event/gpl_and_business/
- Blogpost zu verschiedenen Lizenzen, ihrer Geschichte und Verbreitung, Prototype Fund: https://prototypefund.de/freie-open-source-lizenzen/
- Überblick über Urteile zu Open-Source-Softwarelizenzen, ifrOSS: https://ifross.github.io/ifrOSS/Pages/oss_cases/de#urheberrecht-und-wettbewerbsrecht
- Argumente gegen Contributor License Agreements, Ben Balter (GitHub): https://ben.balter.com/2018/01/02/why-you-probably-shouldnt-add-a-cla-to-your-open-source-project/

□□ Datenschutz

Durch Datenschutz wird das Grundrecht auf die Achtung der Privatsphäre und auf informationelle Selbstbestimmung gewahrt. Zu diesem Zweck definiert das Datenschutzrecht, auf welche Weise personenbezogene Daten – d. h. Daten, durch die Personen identifiziert werden können, wie Namen oder E-Mail-Adressen – verarbeitet werden dürfen.

Datenschutz in der Softwareentwicklung

Das europäische Datenschutzrecht verpflichtet nicht diejenigen, die Software entwickeln und bereitstellen, sondern diejenigen, die personenbezogene Daten mithilfe von Software verarbeiten bzw. für ihre Zwecke verarbeiten lassen. Bei der Entwicklung eines neuen Softwareprojekts ist Datenschutz dennoch von Anfang an wichtig. Denn Software hat nur dann eine Chance eingesetzt zu werden, wenn eine datenschutzkonforme Verarbeitung damit technisch möglich ist.

Entwicklungsprinzipien

Um datenschutzkonforme Software zu entwickeln, sollten zwei Grundprinzipien beachtet werden.

- **Privacy by Design:** Datenschutz durch Technikgestaltung ist ein Designprinzip für die Entwicklung von Software und Hardware, bei der Datenschutzaspekte berücksichtigt werden. Das Ziel ist, dass Software und Hardware von Beginn an alle technischen Voraussetzungen dafür bieten, datenschutzkonform genutzt zu werden, um später zeit- und kostenaufwändige Anpassungen zu vermeiden.
- **Privacy by Default:** Eine besonders wichtige Funktion, die in Software umgesetzt sein sollte, sind datenschutzfreundliche Voreinstellungen. Der Umfang, in dem personenbezogene Daten verarbeitet werden, sollte standardmäßig so gering wie möglich sein und zusätzliche Verarbeitung optional und granular durch Nutzende selbst aktivierbar.

In der Praxis sind folgende Grundsätze und entsprechende Maßnahmen besonders wichtig:

- Datenminimierung:
  Personenbezogene Daten dürfen nur für festgelegte Zwecke und in dafür notwendigem Umfang verarbeitet werden (Art. 5 Abs. 1 lit. b) u. c) DSGVO). Für das Softwaredesign bedeutet das:
  - Software sollte soweit wie möglich **ohne personenbezogene Daten** funktionieren und diese ansonsten, wenn möglich, **lokal speichern**.
  - Im Zweifel sollte die **Verarbeitung optional aktivierbar** sein.
- Speicherbegrenzung:
  Personenbezogene Daten dürfen nur gespeichert werden, so lange sie für den Zweck ihrer

Erhebung benötigt werden (Art. 5 Abs. 1 lit. e) DSGVO). Für das Softwaredesign bedeutet das:
    - Software muss über eine **Löschfunktion** und ggf. eine **Anonymisierungsfunktion** verfügen.
- Richtigkeit, Integrität und Vertraulichkeit:
  Es muss sichergestellt sein, dass personenbezogene Daten sachlich richtig und auf neuestem Stand sind und dass sie vor unbefugter oder unrechtmäßiger Verarbeitung sowie Verlust geschützt sind (Art. 5 Abs. 1 lit. d) u. f) DSGVO). Für das Softwaredesign bedeutet das:
    - Software sollte über **Funktionen für die Aktualisierung und für Backups** von personenbezogenen Daten verfügen.
    - Sie sollte eine **Funktion zur Protokollierung von Änderungen** und **Berechtigungskonzept** anbieten, durch das sich der der Zugriff auf personenbezogene Daten kontrollieren lässt.
    - Eine wirksame Maßnahme, um Integrität und Vertraulichkeit sicherzustellen, ist außerdem die Implementierung von **Verschlüsselung**.
- Betroffenenrechte:
  Personen, deren Daten verarbeitet werden, haben eine Reihe von Rechten. Dazu gehört u. a. das Recht auf Auskunft über die sie betreffende Datenverarbeitung (Art. 15 DSGVO) sowie das Recht auf Datenübertragbarkeit (Art. 20 DSGVO). Für das Softwaredesign bedeutet das:
    - **Transparenz der Verarbeitung** personenbezogener Daten sollte im Vordergrund stehen.
    - Für Nutzendenprofile und damit verbundene Daten sollte eine **Exportfunktion** eingebaut sein.

Relevante Gesetze

Menschenrechte: Ihre Grundlage haben Datenschutzgesetze in den Menschenrechten, die durch die Europäische Menschenrechtskonvention, die Charta der Grundrechte der Europäischen Union und das Grundgesetz garantiert sind.

Datenschutzgrundverordnung (DSGVO): Die DSGVO definiert Grundsätze für die Verarbeitung personenbezogener Daten, die EU-weit unmittelbar gelten.

Bundesdatenschutzgesetz (BDSG): Das BDSG ergänzt die DSGVO in Deutschland und enthält zusätzliche Bestimmungen insbesondere zum Beschäftigtendatenschutz.

Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG): Das TDDDG setzt in Deutschland die ePrivacy-Richtlinie um und regelt unter anderem den Zugriff auf Daten, die auf Geräten von Endnutzenden gespeichert sind, z. B. über das Setzen von Cookies.

Wichtige Organisationen

Datenschutzbehörden: Für die Durchsetzung der DSGVO und des BDSG sind in Deutschland die Datenschutzbehörden zuständig. Die Bundesdatenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben bei Bundesbehörden und Telekommunikationsunternehmen, die Landesdatenschutzbeauftragten sind für öffentliche Stellen der Bundesländer und den nicht-öffentlichen Bereich, z. B. Privatunternehmen oder Vereine, zuständig.

Europäischer Datenschutzausschuss (EDSA): Im EDSA kommen die nationalen Datenschutzbehörden zusammen, um die einheitliche Anwendung der DSGVO sicherzustellen. Dazu gibt das Gremium regelmäßig Leitlinien, Empfehlungen und Best Practices zur Umsetzung der Vorgaben durch die DSGVO.

Stiftung Datenschutz: Die unabhängige Bundesstiftung hat die Aufgabe, Datenschutz in Politik, Wirtschaft, Wissenschaft und Gesellschaft zu fördern. Sie veranstaltet dazu Informations- und Diskussionsveranstaltungen zu Fragen der Datenpolitik und des Datenschutzrechts und stellt praktische Informationen für Zielgruppen wie ehrenamtliche Organisationen oder Kleinunternehmen bereit.

Weiterführende Links

- Ressourcenliste zum Thema DSGVO, Superbloom: https://simplysecure.org/blog/gdpr-resources
- Best Practices für Datenschutz in der Softwareentwicklung, Superbloom: https://simplysecure.org/blog/data-handling
- Guidance on AI and data protection, Information Commissioner‘s Office: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/about-this-guidance/
- Umgang mit besonderen Datenkategorien – Praxisratgeber, Stiftung Datenschutz: https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/besondere-datenkategorien-272

□□ Linksammlung Recht und rechtliche Angelegenheiten

Allgemein

- https://opensource.guide/de/legal/

Lizenzen

- Überblick: https://choosealicense.com/appendix/
- Einführung in die verschiedenen Arten von Lizenzen: https://media.ccc.de/v/ds20-11324-gpl_mit_wtfpl_hah
- Open-Source-Lizenzen und -Businessmodelle: https://archive.fosdem.org/2020/schedule/event/gpl_and_business/
- ifrOSS, Institut für Rechtsfragen der Freien und Open Source Software: https://ifross.github.io/ifrOSS/Pages/licence_center/de
- Übersicht dazu, welche Lizenzen beim Prototype Fund in welchen Projekten genutzt werden, https://prototypefund.de/projects/?filter=dataviz
- Blogpost u. a. zu den Unterschieden zwischen GNU und Copyleft, https://prototypefund.de/freie-open-source-lizenzen/
- Blogpost zu den Eigenheiten der MIT-Lizenz: https://prototypefund.de/mit-lizenz-ftw-oder-nicht/
- Der Licensing Assistant von Interoperable Europe ermöglich es, nach passenden Lizenzen zu suchen und die Kompbalität von verschiedenen Lizenzen zu prüfen: https://interoperable-europe.ec.europa.eu/collection/eupl/solution/licensing-assistant

Datenverarbeitung

- Best Practices für die Datenverarbeitung: https://simplysecure.org/blog/data-handling
- Ressourcenliste zum Thema DSGVO: https://simplysecure.org/blog/gdpr-resources

Datenschutz

- Alexander Lehmann zur DSGVO: https://www.youtube.com/watch?v=gbRuzVwBoLY

- Tobias Deininger, Natalie Dittrich, Softwareentwicklung und Datenschutz – wie passt das zusammen?, https://www.heise.de/hintergrund/Softwareentwicklung-und-Datenschutz-wie-passt-das-zusammen-6155870.html
- Datatilsynet, Software development with Data Protection by Design and by Default, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/
- BSI, IT-Grundschutz-Bausteine, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Überblick Markenrecht - StuFiS

Das Förderprojekt StuFis (Runde 15) hat sich Gedanken dazu gemacht, ob und wie die Marke des Projekts geschützt werden soll. Teammitglied Michelle erläutert im folgenden Beitrag, was das Team in einer Beratung zum Thema lernen konnte.

Beispiele von Marken

Wortmarke: Eines oder mehrere Worte

· Ähnlichkeiten können hier nicht nur in der Schreibweise, sondern auch in der Aussprache bestehen/angemerkt werden.
· Eine Marke darf nicht beschreibend sein (Eierschalensollbruchstellenverursacher wäre z. B, nicht möglich)
· Abkürzungen von Marken sind als eigene Marken anzumelden, wenn man diese schützen möchte.

Wort-/Bildmarke: Der Schutz eines Bildes in Kombination mit einem oder mehreren Worten. Das Wort oder die Wörter sind hier nicht unabhängig vom Bild geschützt.

Entsprechend sollte neben der Wort-/Bildmarke eine Wortmarke angemeldet werden.

Wie funktioniert der Schutz

Die Marke wird in eines oder mehrere Register eingetragen. Das Registeramt überprüft ausschließlich Formalia und keine Ähnlichkeiten. Ein Widerspruch zur Anmeldung durch Dritte kann nur innerhalb einer dreimonatigen Frist erfolgen. Es empfiehlt sich hier, die Register regelmäßig selbst zu durchsuchen oder einen Dienstleister (Stichwort: Markenüberwachung) damit zu beauftragen.

Falls nicht ganz klar ist, ob die Marke „zu beschreibend“ ist, lohnt sich ein Blick in die zurückgewiesenen Marken innerhalb des Registers.

Bei der Eintragung werden international genormte Klassen (
https://www.dpma.de/marken/klassifikation/waren_dienstleistungen/index.html;
https://www.dpma.de/docs/marken/gruppentiteldereinheitlichenklassifikationsdatenbank.pdf)
hinterlegt. Innerhalb dieser Klassen ist die Marke dann geschützt. Sollte jemand mit demselben Wort eine Marke in einer anderen Klasse anmelden wollen, ist das möglich. Daher sollten lieber

mehrere Klassen ausgewählt werden, um möglichst viel abzudecken. Es empfiehlt sich ähnliche Marken im Register zu suchen und dort von den genutzten Klassen inspirieren zu lassen.

Wurde die Marke zunächst z. B. nur in Deutschland angemeldet, hat man sechs Monate Zeit das Anmeldedatum aus Deutschland auch für weitere Register zu verwenden.

Beratungsmöglichkeiten

Das Deutsche Patent- und Markenamt (https://www.dpma.de/index.html) gibt alle wichtigen Informationen zur Anmeldung und Recherche.

Landespatentämter (z. B. Paton in Thüringen) bieten häufig
- kostenlose Beratungsangebote, u. a. auch mit Anwält*innen,
- kostenlose Suche in speziellen Datenbanken, die auch phonetische Recherche ermöglichen.

Auch kostenpflichtige Fachanwält*innen geben natürlich Auskunft (ca. 1.500 – 3.000 EUR).

Kosten für die Anmeldung

Anmeldekosten fallen immer an, auch wenn die Anmeldung abgelehnt/zurückgewiesen wird.

In Deutschland:
- 290 EUR für drei Klassen und zehn Jahre
- Jede zusätzliche Klasse kostet 100 EUR
- Beschleunigtes Verfahren kostet 200 EUR zusätzlich. Anmeldung erfolgt dann innerhalb von sechs Monaten
- Verlängerungsgebühr von 750 EUR

Europaweit:
- 1.000 EUR für Anmeldung in 27 Ländern und 23 Sprachen
- Nur pauschal möglich
- Selbständige Ähnlichkeitsrecherche in allen nationalen Registern notwendig

International:
- In welchen Ländern man anmeldet, ist frei wählbar
- Antrag über das Deutsche Patent- und Markenamt kostet 180 EUR zusätzlich zu den Kosten in den jeweiligen nationalen Registern.

Fördermittel über Finanzhilfeprogramm, das kleinen und mittleren Unternehmen (KMU) in der EU helfen soll, ihre Rechte des geistigen Eigentums zu schützen: https://www.euipo.europa.eu/de/sme-corner/sme-fund/overview.

Verantwortung für Software und Inhalte

Um Anwender*innen vor Risiken durch fehlerhafte Software oder rechtswidrige Inhalte zu schützen, haben diejenigen, die Software verfügbar machen, gewisse Sorgfaltspflichten. Für frei zur Verfügung gestellte Open-Source-Software, die oft in lose organisierten Communities und mit wenig Ressourcen entwickelt wird, gelten nicht alle diese Pflichten in gleicher Weise.

Verantwortung für Open-Source-Software

Wer Open-Source-Software für andere frei, also ohne Bezahlung, verfügbar macht, ist weitgehend von der Haftung für die Software befreit. Der Grund ist, dass das Verfügbarmachen von Open-Source-Software in Deutschland nach vorherrschender Meinung juristisch als Schenkung gilt. Daraus folgt, dass diejenigen, die Open-Source-Software frei verfügbar machen, nur dann für Softwaremängel oder -fehler wie Sicherheitslücken oder Lizenzverstöße haften, wenn sie diese vorsätzlich oder grob fahrlässig verursacht oder arglistig, d. h. bewusst, verschwiegen haben (§§ 521 ff. BGB). Darüber hinausgehende weitgehende Haftungsausschlüsse, wie sie in vielen verbreiteten Open-Source-Lizenzen wie GPLv2 und GPLv3 zu finden sind, könnten in Deutschland unwirksam sein, weil sie gegen AGB-Recht verstoßen. In anderen Ländern können sie dagegen wirksam sein.

Bei der Veröffentlichung von Open-Source-Software sollte man daher

- bei der Wahl der Lizenz ggf. die Wirksamkeit darin enthaltener **Haftungsausschlüsse prüfen**,
- **bekannte Mängel und Fehler beschreiben**,
- so weit wie möglich **auf genutzte Softwarekomponenten sowie deren Lizenzen hinweisen**.

Keine generellen gesetzlichen Ausnahmen von der Haftung gelten dagegen für Personen, die Open-Source-Software bzw. damit verbundene Dienstleistungen wie z. B. Hosting kommerziell anbieten. In welchem Umfang ein Anbieter haftet, hängt von der Art des dafür geschlossenen Vertrags sowie den darin enthaltenen individuellen Vereinbarungen zu Leistungsumfang und Haftungsfragen ab.

In Zukunft kommen durch den Cyber Reslience Act und die Produkthaftungsrichtlinie unter bestimmten Umständen neue Verpflichtungen für Open-Source-Software hinzu.

Verantwortung für Inhalte

Anbieter*innen von digitalen Diensten wie Websites und Plattformen sind für ihre eigenen Inhalte, die sie veröffentlichen, verantwortlich und können bei Verstößen gegen geltendes Recht (z. B. Jugendschutz, Persönlichkeitsrecht, Urheberrecht) haftbar gemacht werden. Das gilt auch, wenn sie sich Inhalte von anderer Stelle zu eigen machen, z. B. indem sie diese nach redaktioneller Prüfung oder Bearbeitung veröffentlichen oder zitieren. Für alle übrigen fremden Inhalte wie User-generated content oder andere gehostete Inhalte haften Anbieter*innen von digitalen Diensten nur bedingt: Wenn sie von einer Rechtsverletzung erfahren, sind sie dazu verpflichtet, die entsprechenden Inhalte umgehend korrigieren zu lassen oder zu löschen (Art. 4 ff. DSA). In der Regel sind keine umfassenden Kontrollen fremder Inhalte erforderlich, um Rechtsverletzungen zu identifizieren.

Generell gilt für Anbieter*innen, die ihre Dienste nicht ausschließlich für private und familiäre Zwecke betreiben, die Pflicht in einem Impressum Kontaktinformationen anzugeben (§ 5 DDG). Bei Diensten, die Inhalte von Nutzenden übermitteln oder in deren Auftrag speichern, muss zudem eine Kontaktstelle für Behörden und Nutzende eingerichtet und die Kontaktdaten leicht zugänglich bekannt gemacht werden (Art. 11f. DSA). Etwaige Regelungen zum Umgang mit fremden Inhalten wie Moderationsrichtlinien sind öffentlich zur Verfügung zu stellen (Art. 14 DSA). Wenn fremde Inhalte gespeichert werden, muss zudem eine Möglichkeit zur Meldung rechtswidriger Inhalte angeboten und im Falle der Löschung von Inhalten eine Begründung an deren Urheber gesendet werden (Art. 16 ff. DSA). Weitergehende Regelungen gelten für Unternehmen ab 50 Beschäftigen und einem Jahresumsatz über 10 Mio. Euro.

Wenn man digitale Dienste anbietet, sind daher folgende Maßnahmen wichtig:

- **sich fremde Inhalte nicht ohne genaue Prüfung zu eigen machen und über fremde Inhalte informieren**, indem man deren Zustandekommen erklärt, klarstellt, dass keine redaktionelle Prüfung oder Bearbeitung der entsprechenden Inhalte stattfindet, und auf Nutzungs- und Verwertungsrechte an ihnen verzichtet
- **Infrastruktur anlegen, um die Meldung rechtswidriger Inhalte zu ermöglichen und bei deren Bekanntwerden schnell reagieren zu können**, indem Urheber um eine Korrektur gebeten oder Inhalte gelöscht werden sowie entsprechende Entscheidungen transparent dargelegt werden

Relevante Gesetze

Bürgerliches Gesetzbuch (BGB): Das BGB definiert sowohl den Haftungsausschluss für Schenkungen als auch die Bedingungen, unter denen Softwareverträge geschlossen und durchgesetzt werden können.

Cyber Resilience Act (CRA): Der CRA legt Sicherheitsanforderungen an Software und Hardware fest. Die Verpflichtungen des CRA gelten für auch für kommerzielle Hersteller und - in abgeschwächter Form – für sogenannte Verwalter von Open-Source-Software, die für kommerzielle Tätigkeiten bestimmt ist. Die ersten Verpflichtungen gelten ab September 2026.

Produkthaftungsrichtlinie (ProdHaftRL 2024): Die neue ProdHaftRL regelt, wann Bereitsteller*innen von Software gegenüber Verbraucher*innen haften. Ausgenommen ist „freie und quelloffene Software, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird“ (Art. 2 Abs. 2 ProdHaftRL). Bis zum 9. Dezember 2026 muss sie in nationales Recht umgesetzt werden.

Digital Services Act (DSA): Der DSA definiert Haftungs- und Sicherheitsvorschriften für digitale Dienste wie z. B. Suchmaschinen, soziale Netzwerke, Messenger oder Cloud-Dienste.

Digitale-Dienste-Gesetz (DDG): Das DDG konkretisiert und ergänzt den DSA, z. B. durch die sogenannte Impressumspflicht und Regelungen zur Durchsetzung des DSA in Deutschland.

Wichtige Organisationen

Bundesnetzagentur: Die Bundesnetzagentur überwacht als sogenannter Digital Services Coordinator in Deutschland die Einhaltung des Digital Services Act.

Weiterführende Links

- Informationen zu Impressum, Haftung und Informationspflichten, IHK München und Oberbayern: https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Internetrecht/
- FAQ zu Haftung und Gewährleistung bei Open-Source-Software, ifrOSS: https://www.ifross.org/?q=category/faq-ordnung/v-haftung-und-gewaehrleistung
- Informationen zur Bedeutung des CRA für Open-Source-Software, OpenSSF: https://openssf.org/category/policy/cra/