



Geistiges Eigentum in der digitalen Welt

Von Online-Shops und Metaverse bis Apps und KI:
So schützen Sie Ihre Ideen, Innovationen und Inhalte

Inhalt

Geistiges Eigentum in der digitalen Welt.	3
Geistiges Eigentum im digitalen Raum – darum geht's!	4
Urheberrecht: Von Fotos im Web über Online-Streams bis zur Künstlichen Intelligenz.	5
Urheberrechtsverletzungen in der digitalen Welt.	6
Werke schützen – drei Tipps.	6
IM FOKUS: Künstliche Intelligenz (KI) und Urheberrecht.	9
Marke und Design zwischen Fake Shop, Metaverse und NFT.	12
Marke und Design im Online-Handel.	13
Marke und Design schützen – drei Handlungsfelder.	14
Geschäftsgeheimnisse schützen.	17
Warum der Schutz so schwierig ist.	18
Drei Tipps zum Schutz Ihrer Geschäftsgeheimnisse.	19
Mehr technische Möglichkeiten – mehr Möglichkeiten für Patente.	21
Patente und die digitale Innovation.	22
Drei Beispiele für Patentschutz in einer digitalen Welt.	23
IM FOKUS: 3D-Druck.	26
Rechte durchsetzen im digitalen Raum.	30
Rechtsverletzungen finden – Monitoring.	31
Illegalen Inhalte online melden – diese Regelungen des Digital Services Act (DSA) sollten Sie kennen.	31
Informationen sammeln mit WHOIS-Abfragen.	35
Das DPMA als digitaler Dienstleister.	36
Glossar.	37

Geistiges Eigentum in der digitalen Welt.

Vom Lernen mit Apps auf dem Smartphone bis zum Verkauf von Produkten oder Dienstleistungen in Online-Shops, vom Augenmerk auf Geschäftsgeheimnisse bis zum 3D-Druck von Ersatzteilen für Maschinen: Geistiges Eigentum in der digitalen Welt ist ein äußerst facettenreiches Thema. Künstliche Intelligenz hat alles noch einmal weitergedreht.

Blick auf geistiges Eigentum aus verschiedenen Perspektiven

Sie möchten einen Überblick gewinnen, wo geistiges Eigentum in der digitalen Welt relevant ist und welche Punkte Sie daher beachten sollten? Diesen Überblick wollen wir Ihnen mit unserer Broschüre geben – ob Sie als Verbraucherin oder Verbraucher oder als Verantwortliche oder Verantwortlicher in einem Unternehmen oder einer Organisation auf die digitale Welt schauen. Wir beantworten Fragen, die Sie sich eventuell stellen: Was heißt geistiges Eigentum in der digitalen Welt eigentlich genau? Und was hat das mit mir zu tun? Was muss ich beachten, um mein geistiges Eigentum im digitalen Raum zu schützen, und was, um die Rechte Dritter nicht zu verletzen?

Die Schattenseiten weltweiter Verfügbarkeit

Digitale Inhalte lassen sich überall auf der Welt abrufen und nutzen. Auch Kopien sind in beliebiger Zahl und verlustfrei möglich. Das gilt für Medieninhalte aller Art, aber auch für Baupläne, Ideen und Rezepturen, die in Sekundenbruchteilen vervielfältigt und verbreitet werden können. So vielseitig und hilfreich die Möglichkeiten der digitalen Welt sind, so schaffen sie doch gleichzeitig die Gefahr, fremdes geistiges Eigentum zu verletzen. Das geschieht häufig unbeabsichtigt, manchmal aber auch mit Vorsatz. So werden etwa in Online-Shops Produkte angeboten und verkauft, die als illegale Nachahmungen Urheber-, Marken-, Patent- oder Designrechte verletzen.

Verschaffen Sie sich einen ersten Überblick

In dieser Situation, die für alle sehr unübersichtlich sein kann, geben wir einen ersten Überblick über das geistige Eigentum in der digitalen Welt. Sie können bei den angegebenen Quellen und Organisationen bei Bedarf weitere Informationen erhalten.

Geistiges Eigentum im digitalen Raum – darum geht's!

Recht des geistigen Eigentums	Definition	Anwendungsbereiche/ Herausforderungen
Urheberrecht	Schützt eine persönliche, geistige Schöpfung	<ul style="list-style-type: none"> • Schutz vor rechtswidriger Nutzung • Metaverse • Generative KI • Software • 3D-Druck
Marke	Schützt die Kennzeichnung von Waren und/oder Dienstleistungen	<ul style="list-style-type: none"> • Schutz vor rechtswidriger Nutzung • Cybersquatting • Fake Shops • Metaverse • Apps
Design	Schützt die Farb- und Formgebung von Erzeugnissen	<ul style="list-style-type: none"> • Metaverse • Fake Shops • Apps • 3D-Druck
Patent/Gebrauchsmuster	Schützen technische Erfindungen	<ul style="list-style-type: none"> • Software • KI-Erfindungen • Apps • 3D-Druck
Geschäftsgeheimnis	Schützt Informationen, die wirtschaftlich wertvoll sind und an deren Geheimhaltung ein berechtigtes Interesse besteht	<ul style="list-style-type: none"> • Cybertheft • 3D-Druck • Software

Zu den aufgeführten Themen erfahren Sie in dieser Broschüre mehr. Wir beantworten die wichtigsten Fragen zu geistigem Eigentum in der digitalen Welt. Die Übersicht und die Darstellungen in der Broschüre sind nicht allumfassend.



Urheberrecht: Von Fotos im Web über Online-Streams bis zur Künstlichen Intelligenz.



Urheberrechtsverletzungen in der digitalen Welt.

Texte, Fotos, Musik oder Filme: Durch die Digitalisierung hat sich die Art und Weise geändert, wie wir urheberrechtlich geschützte Werke nutzen. Damit einher geht die Art und Weise, wie Rechte an diesen Werken verletzt werden können. Urheberrechte sind im Internet besonders gefährdet – und auch die mit ihnen verwandten Leistungsschutzrechte wie der Lichtbildschutz. Letzterer schützt „normale“ Fotos, die keine „Werke“ im Sinne des Urheberrechtsgesetzes (UrhG) sind. Denn ein einfaches Hochladen, Runterladen oder Streamen Ihrer Werke kann im Internet sekündlich ohne Ihre Zustimmung geschehen.

Freischaffende Autorinnen und Autoren, Fotografinnen und Fotografen sowie Content Creators, die mediale Inhalte fürs Internet schaffen, sind aber in der Regel darauf angewiesen, von den Erträgen ihrer Werke zu leben. Entscheidend ist somit, zu kontrollieren, wer Ihre Werke wo und wie unerlaubt nutzt. Mit den folgenden drei Tipps können Sie Ihre Werke erheblich besser vor unerlaubter Nutzung schützen.

Werke schützen – drei Tipps.

1

Legale Nutzungsmöglichkeiten anbieten

Eine Studie des Amts der Europäischen Union für geistiges Eigentum (EUIPO) kam 2023 zum Ergebnis: Wo mehr legale Nutzungsmöglichkeiten für Musik-, Film- und TV-Streams existieren, haben Verbraucherinnen und Verbraucher weniger Anreize, auf illegale Angebote zurückzugreifen.¹ Sorgen Sie daher dafür, dass Verbraucherinnen und Verbraucher Ihr Werk mit gutem Gewissen genießen können. Etwa mittels eines legalen Streamingportals oder einer Kaufmöglichkeit. Mithilfe von Nutzungsbedingungen können Sie den Umfang der Nutzungsmöglichkeiten festlegen.

Sie wollen Ihr Werk der Öffentlichkeit kostenlos zur Verfügung stellen? Dies ist durch sogenannte „Open-Content-Lizenzen“, zum Beispiel standardisierte Creative Commons Lizenzen, möglich. Diese standardisierten Lizenzen ermöglichen Dritten die Nutzung unter bestimmten Voraussetzungen; zum Beispiel Namensnennung oder nur nichtkommerzielle Nutzung oder Nutzung nur in unveränderter Form.

¹ EUIPO, Online copyright infringement in the European Union, 2023, Seite 70 ff.

2

Copyright-Vermerk

Die Angabe eines Copyright-Vermerks ist zwar freiwillig und nicht zwingend notwendig, um Ihre Rechte zu schützen. Dennoch hat ein Copyright-Vermerk, mit dem Sie sich als Urheber oder Rechteinhaberin zu erkennen geben und sich Ihre Rechte am Werk vorbehalten (zum Beispiel „©, Name, Erscheinungsdatum des Werks, all rights reserved“), gleich zwei Vorteile:

Erstens als Warnfunktion, dass dieses Werk nicht ohne Ihre Erlaubnis genutzt werden darf. Zweitens ist für Interessierte so ersichtlich, an wen sie sich für Nutzungsfragen wenden können. Sie können auch auf die Möglichkeit hinweisen, dass Interessierte Sie für die Lizenzierung beispielsweise per E-Mail kontaktieren können, um einen einfachen Weg zur legalen Nutzungsmöglichkeit aufzuzeigen.

3

Digital Rights Management

Digitales RechteManagement (englisch: Digital Rights Management, DRM) bedeutet, digitale Inhalte mit Hilfe von Technik zu schützen. Beispiele sind:

- **Barrieren bauen:** Beschränken Sie den Zugang und die Nutzung Ihres Werks. Etwa durch eine Zugangskontrolle oder einen Kopierschutz. Technische Beschränkungen begegnen Ihnen im Alltag immer wieder. Etwa bei Software oder Computer-Betriebssystemen mittels einer Produktaktivierung. Wirksame technische Maßnahmen dürfen grundsätzlich nicht umgangen werden.
- **Werkkopien mit digitalen Wasserzeichen individualisieren und nachverfolgbar machen:** Wenn Sie online beispielsweise ein Foto zur digitalen Nutzung anbieten, können Sie in der jeweiligen Datei Informationen hinterlegen. Etwa, um die Rechteinhaberin oder den Rechteinhaber, aber auch die Nutzungsbedingungen hinsichtlich dieser speziellen Datei festzuhalten.

Diese Informationen ermöglichen es, Kopien dieser Datei nachzuverfolgen – sogenanntes Tracking. Das ist hilfreich bei der Beweissicherung im Falle einer Urheberrechtsverletzung. Bild-, Text-, Audio- oder Videodateien können mit sichtbaren oder unsichtbaren/unhörbaren Wasserzeichen versehen werden. Bei Letzteren werden minimale Veränderungen am Werk vorgenommen, die für den Menschen nicht wahrnehmbar sind; zum Beispiel Veränderung einiger Pixel, Frequenzänderung. Vom Rechteinhaber zur Wahrnehmung seiner Rechte eingefügte Informationen, wie zum Beispiel Wasserzeichen, dürfen grundsätzlich nicht entfernt oder verändert werden.

In dieser Weise manipulierte Dateien dürfen grundsätzlich nicht wissentlich ohne Befugnis verbreitet, gesendet oder veröffentlicht werden.



- **Urhebereigenschaft und Nutzungsbedingungen mithilfe von NFT nachweisen:** Anfang der 2020-er Jahre gab es einen regelrechten „NFT-Hype“ in der Kunst: Digitale Werke erzielten, versteigert oder verkauft, als sogenannte NFT-Kunstwerke (Non-fungible Token, NFT, auf Deutsch „nicht-austauschbare Wertmarke“) hohe Summen. Zum Beispiel Werke wie die „Bored Ape Yacht Club“-Kollektion oder auch bekannte Meme-Vorlagen wie „Disaster Girl“. Memes sind humorvolle Inhalte, die im Internet vielfach geteilt werden.

Was genau aber bedeutet NFT? „Token“ sind eine Art digitales Zertifikat. NFT sind „non-fungible“, also nicht austauschbar. Das liegt daran, dass NFT mithilfe der Blockchain-Technologie erzeugt und in der Blockchain gespeichert werden. Eine Blockchain wiederum besteht aus Datenblöcken, die so miteinander verbunden sind, dass die Blöcke nicht vertauscht werden können. Der Vorteil dieser Technologie: Sie gilt als sehr sichere Verschlüsselung und somit als wirksames Mittel gegen Manipulationen. Aufgrund dieser Eigenschaften eignen sich NFT, um die Authentizität eines digitalen Werks nachzuweisen oder mit einem Werk zu handeln.

Achtung Verwechslungsgefahr: Nicht das Werk wird in der Blockchain gespeichert, sondern das Zertifikat, das einen als Inhaberin oder Inhaber ausweist. Das bedeutet: Wie bei einem herkömmlichen digitalen Text, Film oder Foto schützt ein NFT nicht vor der faktischen Nutzung. Aber nur wer den NFT – also das Zertifikat – besitzt, hat auch die Rechte am Werk. Das gilt nicht nur im Urheberrecht. Deshalb spielen NFT auch eine Rolle, wenn es um den Marken- und Designschatz beispielsweise im Metaverse geht (siehe Seite 15).

Übrigens:

Mehr über Digital Rights Management erfahren Sie unter anderem im **Anti-Counterfeiting and Anti-Piracy Technology Guide** des Europäischen Amts für geistiges Eigentum:

💻 <https://euipo.europa.eu/anti-counterfeiting-and-anti-piracy-technology-guide/>



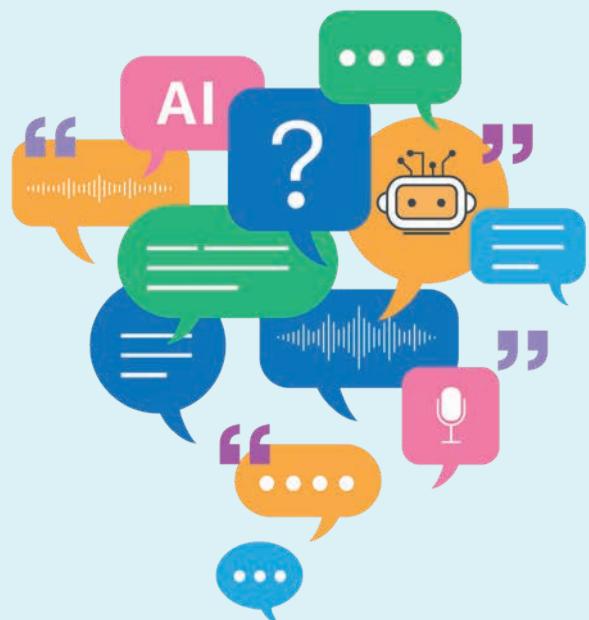
Künstliche Intelligenz (KI) und Urheberrecht.

Künstliche Intelligenz ist längst von einer Zukunftsvision zu einer Alltagstechnologie geworden. Sie findet sich in Saugrobotern oder Fahrassistentensystemen, in Helfern für den Alltag. Besondere Aufmerksamkeit hat das Thema KI durch neue Programme wie ChatGPT, Gemini oder LeChat erfahren: Mit sogenannter generativer Künstlicher Intelligenz können in Sekundenschnelle und teilweise kostenlos Texte oder Bilder erstellt werden. Dabei entstehen zahlreiche Fragen zum Urheberrecht:

Ist mein durch KI erstellter Inhalt geschützt?

Ein von einer KI erstellter Inhalt, sogenannter „Output“, ist nicht urheberrechtlich geschützt, wenn er vollständig durch eine KI erzeugt wurde. Schwieriger ist der Fall zu beurteilen, wenn die KI lediglich als Werkzeug eingesetzt wird.

Zum Hintergrund: Auch bei KI-generierten Inhalten gilt das klassische Urheberrecht. Das bedeutet: Wie bei herkömmlich erstellten Texten, Bildern, Musikstücken oder Filmen auch, ist ein Werk dann urheberrechtlich geschützt, wenn es eine persönliche, geistige Schöpfung ist. Persönliche Schöpfung bedeutet, dass ein Mensch das Werk geschaffen haben muss. Bei Output, der vollständig durch eine KI generiert wurde, hat die KI und kein Mensch den Inhalt geschaffen. Es handelt es sich also nicht um eine persönliche Schöpfung. Die Folge: Der neu erstellte Inhalt ist nicht als Werk urheberrechtlich geschützt. Schwieriger zu beantworten ist die Frage, wenn der Output nicht von, sondern mithilfe einer KI produziert wird. Insoweit ist die Antwort auf die Frage, ob der Output als persönliche Schöpfung urheberrechtlich geschützt ist, vom Einzelfall abhängig.



Was muss ich beim Verwenden meiner mit KI erstellten Inhalte beachten?

Auch hier bleibt es rein rechtlich bei den gewöhnlichen urheberrechtlichen Vorschriften: Wer ein Werk schafft und dieses nutzen will, sei es durch Kopieren, Verkaufen oder Veröffentlichen im Internet, muss darauf achten, keine bestehenden Rechte Dritter zu verletzen. Beispielsweise kann die Nutzung eines KI-generierten Outputs Urheberrecht verletzen, wenn der Output ein bereits bestehendes Bild oder einen Text wiedergibt oder diesen stark ähnelt. Finden die Inhaberinnen und Inhaber von Rechten ihre Werke in einem KI-generierten Output wieder, dann können sie gegen die Nutzung vorgehen und etwa Unterlassung oder unter Umständen Schadensersatz fordern. Denn die Nutzung solcher urheberrechtlich geschützter Inhalte bedarf grundsätzlich der Zustimmung der Rechteinhaberin oder des Rechteinhabers.



Was gilt für das Trainieren von KI-Modellen?

Nicht immer ist beim Training von KI-Modellen geistiges Eigentum betroffen. So sind zum Beispiel Daten an und für sich nicht urheberrechtlich geschützt. Anders liegt der Fall, wenn die Daten beispielsweise einer urheberrechtlich geschützten Datenbank entstammen oder selbst als Text, Foto oder Musikstück urheberrechtlich geschützt sind.

Hinsichtlich des Trainings von KI-Modellen in Deutschland sind insbesondere das UrhG sowie die KI-Verordnung (KI-VO) zu beachten:

- Grundsätzlich zulässig ist gemäß § 44b UrhG das Erstellen von Trainingsdatensätzen als Text und Data Mining. Das meint Vervielfältigungen von rechtmäßig zugänglichen digitalen und digitalisierten Werken für die automatisierte Analyse, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen. Text und Data Mining ist nicht erlaubt, wenn der Rechtsinhaber oder die Rechtsinhaberin einen Nutzungsvorbehalt ausgesprochen hat (sogenannter Opt-out). Das Urheberrecht kennt noch eine weitere Erlaubnis für Text und Data Mining speziell für wissenschaftliche Forschung: § 60d UrhG. Hiernach dürfen zum Beispiel Forschungseinrichtungen wie Hochschulen, aber auch öffentlich zugängliche Bibliotheken und Museen Text und Data Mining unter bestimmten Voraussetzungen durchführen. Zum Zweck der wissenschaftlichen Forschung im Sinne des § 60d UrhG ist Text und Data Mining trotz eines Nutzungsvorbehalts erlaubt.
- Anbieter von General Purpose AI-Modellen – also Systemen, die für eine Vielzahl von Aufgaben wie Text- und Bildgenerierung oder Problemlösung eingesetzt werden können – müssen außerdem eine hinreichend detaillierte Zusammenfassung erstellen und veröffentlichen, welche Inhalte zu Trainingszwecken verwendet wurden (Art. 53 I d) KI-VO). Sie müssen auch eine Strategie zur Einhaltung des europäischen Urheberrechts entwickeln (Art. 53 I c) der KI-VO).

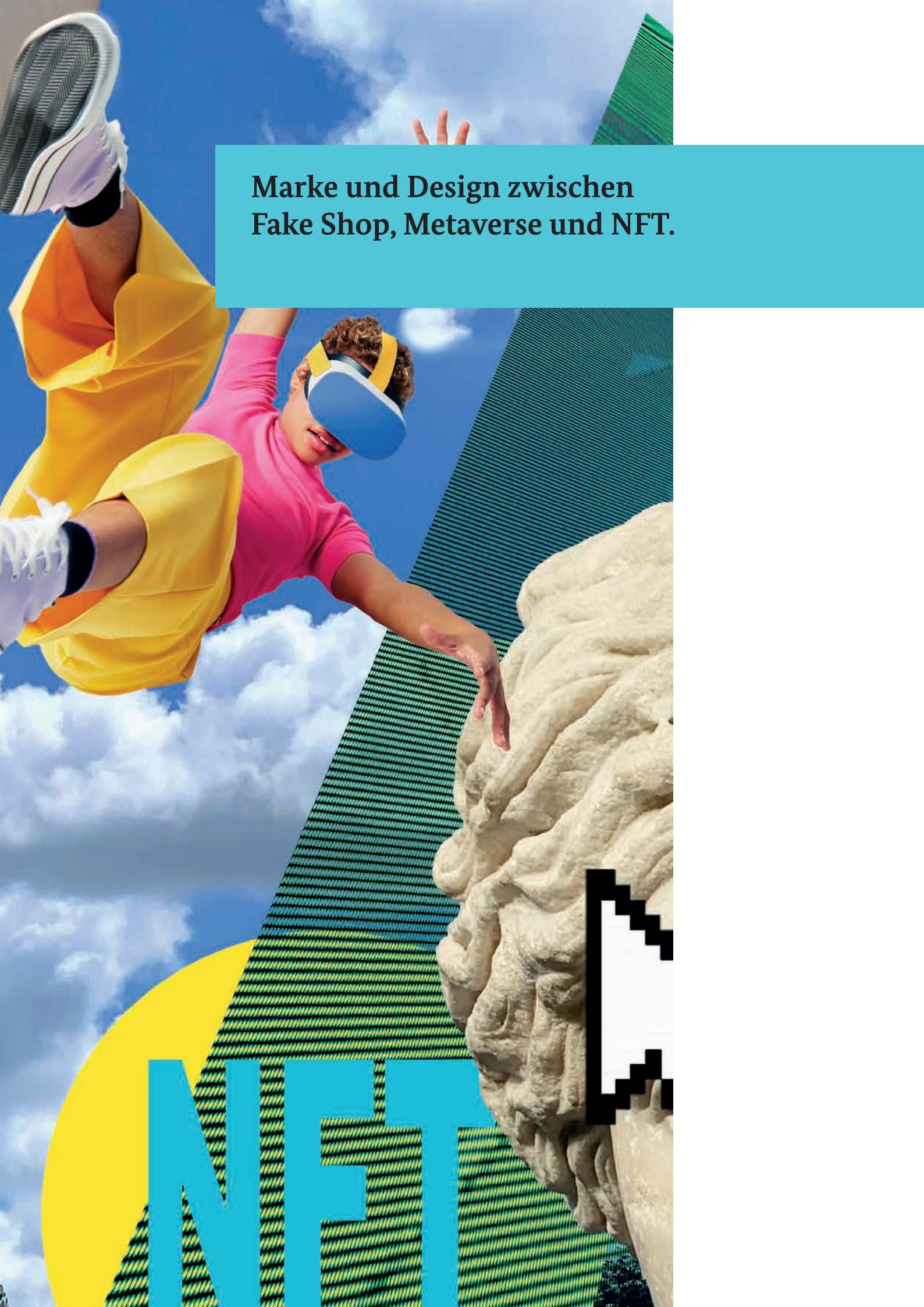
Diese Broschüre gibt den Stand zum Zeitpunkt des Redaktionsschlusses wieder.

Wichtig ist auch: Das Thema KI ist nicht weltweit harmonisiert. Unterschiedliche Länder der Welt können den Schutz von KI-Inhalten daher auch verschieden bewerten. Als Deutsches Patent- und Markenamt geben wir hier die deutsche Perspektive wieder.

Mehr zum Thema KI und Urheberrecht erfahren Sie in der Studie des EUIPO:

- 💻 <https://www.euipo.europa.eu/en/news/euipo-releases-study-on-generative-artificial-intelligence-and-copyright>





A collage of images illustrating the intersection of fashion, technology, and art. It features a person in a yellow tracksuit performing a high kick, a person wearing a VR headset interacting with a classical statue, a large yellow circle containing the letters 'NFT', and a modern skyscraper against a blue sky.

Marke und Design zwischen
Fake Shop, Metaverse und NFT.

Marke und Design im Online-Handel.

Wie im analogen Handel besteht auch im Online-Handel ein Problem mit Marken- und Produktpiraterie. Nachgeahmte Markenware lockt Verbraucherinnen und Verbraucher mit Schnäppchenpreisen. Nicht selten wird sich dabei sogar fremder Produktfotos bedient – soweit keine Einräumung entsprechender Nutzungsrechte vorliegt, werden somit auch Urheberrechte oder Leistungsschutzrechte verletzt.

Im grenzüberschreitenden (Online-)Handel besonders wichtig: Marken und Designs gewähren Schutz grundsätzlich nur im Land der Eintragung. Es gilt das Territorialitätsprinzip. Möchten Sie gegen Rechtsverletzungen vorgehen, sollten Sie daher zunächst prüfen, ob Ihre Marke oder Ihr Design im jeweiligen Land Schutz genießt. Bei internationalen Registrierungen (EU- und IR-Marken sowie EU- und IR-Designs) ist zu prüfen, ob der Schutz territorial gilt oder auf das jeweilige Land wirksam erstreckt wurde.

Unter Umständen können aber auch Online-Angebote aus dem Ausland Ihr geistiges Eigentum nach deutschem Recht verletzen. Ob Marke oder Urheberrecht: Ist das Angebot oder die Nutzung des Werks nicht klar auf den deutschen Markt ausgerichtet (beispielsweise durch die Nutzung einer deutschen Top-Level-Domain „.de“ mit Angeboten in deutscher Sprache), sondern liegt der Schwerpunkt im Ausland, muss geprüft werden, ob es einen hinreichenden **wirtschaftlich relevanten Inlandsbezug** gibt, einen sogenannten „**commercial effect**“.² Ob ein solcher Bezug zu Deutschland vorliegt, muss unter Berücksichtigung der Interessen und Umstände im Einzelfall abgewogen werden.



² Dies hat der BGH zum Marken- und zum Urheberrecht entschieden, vgl. zur Marke BGH, Urteil vom 7. November 2019, Az. I ZR 222/17, zum Urheberrecht BGH, Urteil vom 5. Dezember 2024, Az. I ZR 50/24.

Marke und Design schützen – drei Handlungsfelder.

Achtung: Cybersquatting!

Beim **Cybersquatting** missbrauchen Dritte den guten Ruf einer Marke und lassen die noch nicht vom Markeninhaber besetzten Domain-Namen registrieren, die einen Markennamen enthalten, um Nutzerinnen und Nutzer auf diese Seite zu locken oder diese Domain teuer zu verkaufen. Weit verbreitet ist zudem das sogenannte **Typosquatting**: Die Nutzung des Kennzeichens erfolgt mit kleinen Rechtschreibfehlern („typos“ – englisch für Tippfehler). Unser Tipp: Handeln Sie proaktiv und lassen Sie Domain-Namen, die Ihre Marke enthalten, frühzeitig, möglichst zeitgleich mit der Markenanmeldung, registrieren, damit Dritte Ihnen nicht zuvorkommen. Also neben www.beispiel123.de etwa auch www.beispiel123.eu und www.beispiel123.com.

Cybersquatting kann zudem im Zusammenhang mit sogenannten **Fake Shops** stehen. Betrügerinnen und Betrüger kopieren hierbei den Webauftritt von Marken- oder Designinhaberinnen und -inhabern und werben mit vermeintlicher Originalware zu günstigen Preisen. Wer hier bestellt, erhält oft keine Ware für sein Geld. Helfen Sie anderen: Sind Sie als Marken- und/oder Designinhaber oder Verbraucher von einem Fake Shop betroffen, stellen Sie nicht nur Strafantrag bei der Polizei, sondern melden Sie den Shop auch den Verbraucherzentralen. So können andere Verbraucherinnen und Verbraucher mithilfe des Fake Shop-Finders gewarnt werden. Sie (oder auch ein Trusted Flagger) können den Shop auch dem Anbieter melden, der die Webseite hostet (siehe Seite 33).



https://www.polizei.de/Polizei/DE/Einrichtungen/Onlinewache/onlinewache_node.html



<https://www.verbraucherzentrale.de/beschwerde>



<https://www.verbraucherzentrale.de/fakeshopfinder-71560>



Keine Markeneintragung durch Register privater Unternehmen

Einige E-Commerce-Plattformen bieten an, eine Marke in ihren unternehmens-eigenen „Marken-Registern“ eintragen zu lassen. Damit sollen nach Angaben dieser Plattformen Marken leichter vor Nachahmung und Missbrauch geschützt werden. Eine Eintragung in solche Register ist grundsätzlich nicht schädlich, ersetzt aber nicht die Registrierung in einem amtlichen Register, zum Beispiel des DPMA. Wenn Sie Ihre beim DPMA registrierte oder zur Registrierung ange-meldete Marke zusätzlich in einem solchen privatrechtlichen Register anmelden, sollten Sie daher weiter Ihre amtlich eingetragene Marke im Auge behalten und diese rechtzeitig verlängern, um weiterhin Schutz zu genießen.

Marken- und Designschutz im Metaverse

Metaverse – was ist das eigentlich genau?

Eigentlich gibt es gar nicht ein Metaverse, sondern viele! Denn „das“ Metaverse besteht aus vielen digitalen Welten, in denen Avatare, also Kunstfiguren, virtuell zusammenkommen und miteinander interagieren können. Die Userin oder der User fühlt sich mithilfe einer VR-Brille („Virtual reality“) wie mitten im Ge-schehen oder es werden mithilfe einer AR-Brille („Augmented reality“) virtuelle Elemente in die analoge Realität eingeblendet. Und inzwischen sind Metaversen auch ohne Hilfsmittel erlebbar. Anwendungsbeispiele sind etwa Videospiele oder Arbeitsräume für virtuelle Meetings.

Einige namhafte Marken und Designs sind in verschiedenen Metaversen vertre-tten. Wie unsere reale Welt kann auch das Metaverse Marktplatz für den Handel mit (digitaler) Markenware und Designprodukten sein, etwa Kleidung oder Einrichtungsgegenständen für Avatare. Somit können im Metaverse auch Ihre Rechte des geistigen Eigentums (insbesondere Marken, Designs und Urheber-rechte) verletzt werden.



Ihr Schutz des geistigen Eigentums – rechtlich und technisch

Auch im Metaverse können Sie Ihr geistiges Eigentum schützen:

- **Eintragung:** Wer im Metaverse Waren anbietet, kann sich nicht einfach auf seine für die reale Welt geschützten Warenklassen stützen: Denn virtuelle Waren sind im Grunde Programmcodes, also digitale Produkte der Klasse 9 der Nizza-Klassifikation. Designs können bislang unter der Locarno-Klassifikation 14-04 („Grafische Benutzeroberflächen und Icons“) angemeldet werden. Unter Umständen bieten sich im Metaverse auch der Schutz zusätzlicher Klassen an (in Bezug auf Marken zum Beispiel für Dienstleistungen in den Klassen 35, 36, 41 oder 42) – eine Schutzrechtsstrategie sowie eine gute Recherche sind daher sowohl in der analogen als auch in der digitalen Welt Ihr Schlüssel zum Erfolg!
- **Technik:** Mithilfe sogenannter Non-Fungible-Tokens (NFT), einer Blockchain-Technologie, die bestimmte Informationen in der Blockchain manipulations-sicher speichern kann, können Sie sicher mit Ihren digitalen Gütern handeln, indem die Authentizität der Ware nachweisbar ist oder Sie Ihre Inhaberschaft an einem virtuellen Gut nachweisen können.
- **Mehr Schutz im Metaverse durch ein neues Design-Recht:** Derzeit erfährt das Designrecht ein Update – mittels einer EU-Verordnung sowie einer Design-Richtlinie. Die Richtlinie muss bis zum 9. Dezember 2027 von den Mitgliedsstaaten umgesetzt werden. Sie enthält einige Neuerungen und Klarstellungen: Zum Beispiel, dass auch unkörperliche Designs geschützt werden können, etwa Bewegungen, Hologramme, Lichtdesigns. Das deutsche Design-Recht ist hierfür bereits gut gewappnet: Durch den nicht abschließenden Design-Katalog sind schon heute solche Anmeldungen möglich.

Praxistipp:

Formulierungen in Warenverzeichnissen könnten beispielsweise lauten:
„herunterladbare virtuelle Bekleidung“ oder „herunterladbare Computersoftware für Blockchain-Technologie“

Geschäftsgeheimnisse
schützen.



Warum der Schutz so schwierig ist.

Heutzutage werden Geschäftsgeheimnisse zunehmend durch illegale Zugriffe auf Computer und Rechnernetze gestohlen. Wenn vertrauliche Informationen in die Hände von Wettbewerbern oder der Öffentlichkeit gelangen, kann dies Ihrem Unternehmen schaden.

Schätzungen zufolge gehen durch Cyber-Diebstahl in der EU rund 60 Milliarden Euro an Umsatz pro Jahr verloren, 289.000 Arbeitsplätze sind gefährdet.³

Ein Geschäftsgeheimnis ist im Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) – vereinfacht ausgedrückt – definiert als eine Information, die

- (1) nicht allgemein bekannt ist,
- (2) von wirtschaftlichem Wert für ihren Inhaber ist,
- (3) deren Inhaber ein berechtigtes Interesse an ihrer Geheimhaltung hat,
- (4) und deren Inhaber angemessene Schutzmaßnahmen zur Geheimhaltung dieser Information vorgenommen hat.

Der Schutz von Geschäftsgeheimnissen ist eine wichtige Aufgabe, die eine Kombination aus rechtlichen, technischen und organisatorischen Maßnahmen erfordert. Gerade in einer digital vernetzten Welt ist es für Unternehmen wichtiger denn je, ihre wertvollsten Daten zu schützen. In einem ersten Schritt sollten Sie dazu sensible Informationen, die geschützt werden müssen, identifizieren und klassifizieren, um sicherzustellen, dass Informationen entsprechend ihres Sensitivitätslevels kategorisiert werden und entsprechend ihres Risikos vor unberechtigter Offenlegung oder Zugriff geschützt werden können.



³ https://single-market-economy.ec.europa.eu/news/european-commission-launches-cyber-theft-prevention-toolkit-protect-smes-trade-secrets-high-risk-2024-10-15_en

Drei Tipps zum Schutz Ihrer Geschäftsgeheimnisse.

1

Rechtlicher Schutz durch Geheimhaltungsvereinbarungen

Auch im digitalen Raum verhindern wirksame Geheimhaltungsvereinbarungen, dass vertrauliche Daten missbraucht oder ohne Ihre Zustimmung verwendet werden. Geschäftsgeheimnisse reichen von Herstellungsverfahren über Kundenlisten bis hin zu Rezepten und Algorithmen. Diese Informationen sind häufig wichtig, um Wettbewerbsvorteile zu sichern.

Wichtig:

Nutzen Sie bereits frühzeitig entsprechende Geheimhaltungsvereinbarungen, beispielsweise bei der Anbahnung von Geschäftsbeziehungen, bei der Zusammenarbeit mit Ihren (nicht nur externen) Partnern und Beschäftigten. Vergessen Sie nicht, auch Regelungen in Altverträgen zu überprüfen.

2

Organisatorischer Schutz durch Need to know-Prinzip und Sensibilisierung

Achten Sie darauf, Geschäftsgeheimnisse nur einem begrenzten Personenkreis zugänglich zu machen. Dieses Vorgehen wird vielfach auch unter der Bezeichnung „Need to know-Prinzip“ behandelt. Es besagt, dass nur die Personen Zugang zu bestimmten Informationen erhalten sollten, die diese Informationen wirklich benötigen, um ihre Arbeit erfolgreich ausführen zu können. Mit entsprechenden Maßnahmen für den Datenzugriff werden daher vertrauliche Informationen wirksamer vor potenziellen Bedrohungen geschützt und die Anfälligkeit für Cyberangriffe und interne Datenverstöße verringert.

Neben Cyber-Risiken bestehen auch Gefahren, die nicht aus kriminellen Aktivitäten herrühren. Dazu zählen beispielsweise technisches Versagen, etwa Hardware-Defekte oder Software-Fehler, aber auch menschliches Versagen, wie beispielsweise das Verlieren von Datenträgern oder das versehentliche Veröffentlichen von Informationen. Schulungen zum Geheimnisschutz schaffen Bewusstsein und sensibilisieren Ihre Mitarbeiterinnen und Mitarbeiter zusätzlich.

3

Technischer Schutz durch angepasste IT-Infrastruktur

Cyberangriffe sind vorsätzliche Versuche, Daten, Anwendungen oder andere für den geschäftlichen Erfolg relevante Informationen, beispielsweise Geschäftsgeheimnisse, durch unbefugten Zugriff auf ein Netzwerk, ein Computersystem oder ein digitales Gerät zu stehlen, offenzulegen, zu verändern, zu deaktivieren oder zu zerstören.

Laut einer Bitkom-Studie⁴ waren 74 Prozent der Firmen in Deutschland mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr in 2024 von Datendiebstahl betroffen – und im Zuge der fortschreitenden Digitalisierung wird diese Zahl vermutlich weiter ansteigen. Das Ausspähen von Geschäftsgeheimnissen und Datenschutzverletzungen durch Phishing wird zunehmend als Problem erkannt.

Beim Phishing (ein Neologismus für *fish*, deutsch *angeln*) werden häufig irreführende E-Mails an ahnungslose Mitarbeiterinnen und Mitarbeiter geschickt, die die gefährlichen Anhänge öffnen. Auf diese Art versuchen Hacker, Login-Daten zu stehlen und sich Zugriff auf das Unternehmensnetzwerk zu verschaffen. Das macht es den Angreifern auch möglich, Geschäftsgeheimnisse auszuspähen.

Am schwersten trifft es die kleinen und mittleren Unternehmen (KMU). Denn: Während Großunternehmen eigene IT-Abteilungen und umfangreiche Sicherheitsvorkehrungen vorhalten, sind KMU oft nicht ausreichend auf Cyber-Angriffe vorbereitet und unterschätzen vielfach die Bedrohung für den eigenen Betrieb. Häufig fehlen Zeit oder Ressourcen, um sich im nötigen Umfang abzusichern.

Schutz gegen Cyber-Risiken – Machen Sie Ihr Unternehmen fit im Kampf gegen Cybertheft!

Um kleine und mittlere Unternehmen dabei zu unterstützen, ihre Cyberresilienz zu erhöhen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit Partnern den CyberRisikoCheck entwickelt. Er ermöglicht insbesondere Klein- und Kleinstunternehmen eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus und zeigt auf, welche konkreten Maßnahmen ein Unternehmen umsetzen oder bei einem IT-Dienstleister beauftragen sollte.

Das Europäische Amt für geistiges Eigentum bietet ein ganzes Toolkit mit Informationen, FAQ, Fallstudien und Trainings rund um das Thema Cybersicherheit an – bald auch in deutscher Sprache:

- 💻 <https://euipo.europa.eu/knowledge/course/view.php?id=5253>



Viele weitere Informationen zum Thema erhalten Sie auch im Leitfaden „Cybersicherheit für KMU“ des BSI.

- 💻 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cybersicherheit_KMU.pdf?__blob=publicationFile&v=15



- 💻 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cybersicherheit_KMU.html



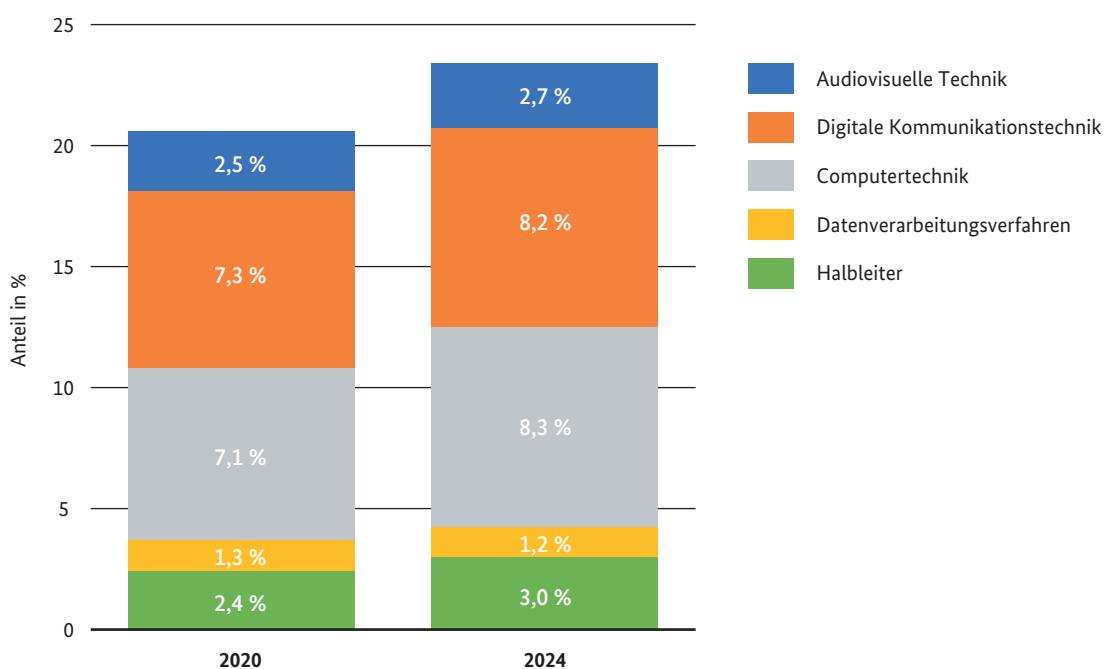
⁴ Bitkom e.V., Studie Wirtschaftsschutz 2024, 2024, Seite 8: <https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz>.



Mehr technische Möglichkeiten –
mehr Möglichkeiten für Patente.

Patente und die digitale Innovation.

Anteil der Patentanmeldungen in ausgewählten Gebieten der Digitalisierung an allen Patentanmeldungen mit Wirkung für Deutschland



Anmerkungen: Abbildung enthält von DPMA und EPA veröffentlichte Anmeldungen unter Vermeidung von Doppelzählungen. Technologiefelder gemäß WIPO IPC-Technologie Konkordanztabelle, verfügbar unter: www.wipo.int/ipstats/en/index.html#resources. Zum Abfragezeitpunkt gültige IPC-Klassen anteilig gezählt. Kein Anspruch auf Vollständigkeit. Ergebnisse ohne Bezug zu Digitalisierung können enthalten sein.

Innovation treibt den digitalen Wandel voran – und gleichzeitig verändert die Digitalisierung die Art und Weise, wie Innovationen entstehen. Sie bestehen zunehmend nicht mehr nur aus Hardware, sondern auch aus Algorithmen, Software und Künstlicher Intelligenz. Das spiegelt sich unter anderem in der Patentstatistik wider (siehe Abbildung oben). Mit der wachsenden Zahl Software- und KI-basierter Erfindungen stellt sich die Frage, in welchem Umfang ein umfassender Patentschutz für digitale Innovationen möglich ist.

Drei Beispiele für Patentschutz in einer digitalen Welt.

Software und computerimplementierte Erfindungen

Software und Computerprogramme als solche, beispielsweise als ausführbare „EXE“-Datei auf einem Computer, einem USB-Stick oder einer CD/DVD, sind nicht patentierbar, sondern können unter den Schutz des Urheberrechts (Schutz für Computerprogramme, § 69a UrhG) fallen.

Dagegen können Erfindungen, die einen Bezug zu Geräten und Verfahren der elektronischen Datenverarbeitung haben, als sogenannte programmbezogene oder computerimplementierte Erfindungen patentfähig sein. Diese müssen auf technischen Überlegungen beruhen und ein technisches Problem lösen.

Nach gefestigter BGH-Rechtsprechung ist die Prüfung der Patentierbarkeit von computerimplementierten Erfindungen nach einem dreistufigen Prüfungsansatz vorzunehmen. Das **erste Kriterium** ist gemäß § 1 Abs. 1 PatG die Technizität, die einen technischen Charakter der Erfindung verlangt. Dieses Kriterium ist in der Regel schon gegeben, wenn die Erfindung auch nur implizit die Nutzung einer Datenverarbeitungsanlage lehrt. Da Computerprogramme als solche jedoch vom Patentschutz ausgeschlossen sind,⁵ muss eine computerimplementierte Erfindung ein **zweites Kriterium** erfüllen. Demnach muss die beanspruchte Lehre Anweisungen enthalten, die der Lösung eines konkreten technischen Problems mit technischen Mitteln dienen.⁶ Nach dem **dritten Kriterium** schließlich ist die computerimplementierte Erfindung auf Neuheit und erforderliche Tätigkeit gegenüber dem Stand der Technik zu prüfen,⁷ wobei nur diejenigen Aspekte der Erfindung zu berücksichtigen sind, die die Lösung des konkreten technischen Problems mit technischen Mitteln bestimmen oder zumindest beeinflussen.

Welche Erfindung erfüllt das Kriterium „Lösung eines technischen Problems mit technischen Mitteln“?

Nicht patentierbar 	Patentierbar 
Neue Darstellungsweise aufgrund von Fahrposition bei Navigationsgerät	Steuerung von Geräten (zum Beispiel bei einer Waschmaschine oder das Antiblockiersystem im Auto)
Bloße Erfassung, Speicherung oder Aufbereitung von Daten (zum Beispiel im Fall des Wiederfindens von Informationsseiten im Internet)	Einsparung von Ressourcen (Strom oder Speicherplatz, zum Beispiel Komprimierung von Videos)
Software zur Ermittlung des besten Anschaffungszeitpunktes eines Gerätes führt zur Verbesserung der Rentabilität	Anpassung der internen Funktionsweise des Computers (zum Beispiel Maßnahmen zur Boot-Integrität, die einen erweiterten Schutz während des Systemstarts bieten)

⁵ Gemäß § 1 Abs. 3 Nr. 3 und Abs. 4 PatG (beziehungsweise Art. 52 Abs. 2 Buchst. c und Abs. 3 EPÜ).

⁶ BGH, Urteil vom 26. Oktober 2010, Az. X ZR 47/07.

⁷ Gemäß §§ 3 und 4 PatG.

Ein europäischer Richtlinievorschlag zur gesetzlichen Harmonisierung computerimplementierter Erfindungen scheiterte im Jahr 2005, da das Europäische Parlament eine entsprechende Änderung ausdrücklich ablehnte. Dies führte jedoch zu einer anhaltenden Debatte über die Patentierbarkeit von Software. Kritiker des Patentschutzes argumentieren, dass patentierte Software den Zugang zu Innovationen erschwert. Befürworter des Patentschutzes hingegen betonen, dass in Ländern wie China, Japan und den USA die Patentierbarkeit von Software stärker ausgeprägt ist. Dies könnte langfristig zu einem Wettbewerbsnachteil für Europa führen.

Apps

Ob ein kleines Unternehmen Termin- und Informationsdienste bereitstellt oder ein Start-Up innovative Lernmethoden, kreative Spielideen oder neue technische Lösungen anbietet: Hinter einer App kann eine Menge Erfindungsreichtum stecken. Apps sind Anwendungen (englisch: Applications), spezielle Softwareprogramme, für mobile Geräte wie Smartphones oder Tablets. Eine App, die mithilfe eines Computers implementiert ist, kann als computerimplementierte Erfindung (CII) patentiert werden, wenn sie Anweisungen enthält, die der Lösung eines konkreten technischen Problems mit technischen Mitteln dienen. Der reine Quellcode oder Algorithmus einer App reicht für eine Patentierung also nicht aus, sondern entscheidend ist die technische Funktionalität zur Lösung eines technischen Problems. Ist dies erfüllt, ist eine Patenterteilung grundsätzlich möglich, sofern auch die weiteren gesetzlichen Anforderungen an eine Patenterteilung, beispielsweise hinsichtlich Neuheit und erforderlicher Tätigkeit, erfüllt sind. Beispiele von Patenten in der App-Welt sind Fotofiltertechnologien von Snapchat oder die Musikerkennung von Shazam.

Die meisten Entwickler von Apps, die keine neuen ausgeklügelten technischen Lösungen anbieten, sondern beispielsweise ihre bestehenden Angebote um digitale Dienste erweitern wollen, werden vor allem im Markenschutz eine Form finden, ihre mobile App-Idee zu schützen. Die konkrete grafische Gestaltung der Benutzeroberfläche oder von visuellen Wegweisern kann auch durch das Design schutzfähig sein.



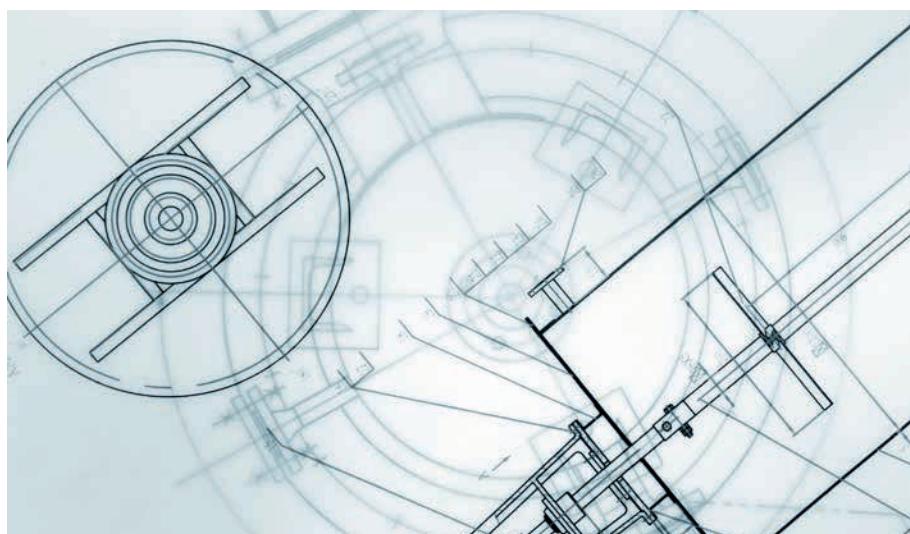
Technische Erfindungen mit KI-Bezug

Mit den Fortschritten in der Künstlichen Intelligenz wächst ihr Einfluss auf den Innovationsprozess und KI trägt zunehmend zur Entwicklung neuer Erfindungen bei. Erfindungen mit einem Bezug zu Künstlicher Intelligenz können Erfindungen sein, die Grundlagen schaffen, um Künstliche Intelligenz anzuwenden oder einzusetzen, oder sie können Erfindungen sein, bei denen Künstliche Intelligenz für ein bestimmtes Anwendungsgebiet oder einen bestimmten Anwendungsfall eingesetzt wird.

KI-bezogene Erfindungen sind nicht grundsätzlich von der Patentierbarkeit ausgeschlossen. Da KI-bezogene Erfindungen in aller Regel eine große Nähe zu computerimplementierten Erfindungen aufweisen, wird für deren Prüfung die Herangehensweise bei programmbezogenen Erfindungen regelmäßig übernommen.

Auch wenn die Fähigkeiten der Künstlichen Intelligenz immer weiter zunehmen und ihr Anteil am Entstehen einer Erfindung mehr und mehr zunimmt, kann ein KI-System – zumindest derzeit – bei allen großen Patentämtern – darunter beispielsweise das Europäische Patentamt und die Patentämter aus Deutschland, den USA, Großbritannien und Korea – nicht als Erfinder eines Patents benannt werden.

Das Bundespatentgericht und der Bundesgerichtshof bestätigten 2021 und 2024,⁸ dass nach deutschem Patentrecht eine KI keine Rechtspersönlichkeit ist und keine Rechtsfähigkeit besitzt. „Ein maschinelles, aus Hard- oder Software bestehendes System kann auch dann nicht als Erfinder benannt werden, wenn es über Funktionen künstlicher Intelligenz verfügt.“ Das US-Höchstgericht kommt zum selben Schluss und erläutert die Entscheidung in den USA damit, dass Patente den menschlichen Einfallsreichtum fördern und belohnen sollen. Daher kann Patentschutz nur für Erfindungen beantragt werden, an denen eine natürliche Person einen wesentlichen Beitrag geleistet hat.



⁸ BPatG, Beschl. v. 11. November 2021, Az. 11 W (pat) 5/21 und BGH, Beschl. v. 11. Juni 2024, Az. X ZB 5/22.

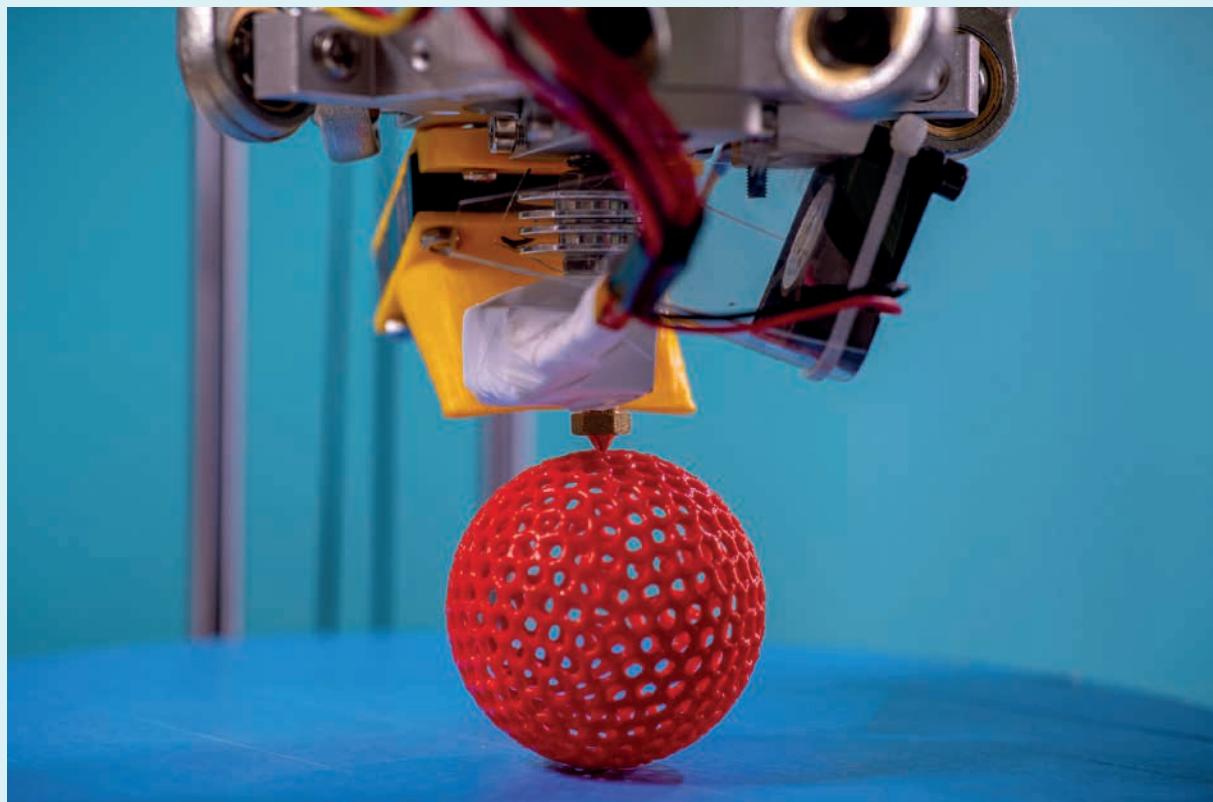
3D-Druck.

Was ist eigentlich ein 3D-Druck?

Ein **3D-Druck** oder **additive Fertigung** bezeichnet Fertigungsverfahren, bei denen Material Schicht für Schicht aufgetragen wird, um dreidimensionale Gegenstände (Werkstücke) zu erzeugen.

Deutschland als Europameister

Die additive Fertigung hebt die traditionellen technischen Beschränkungen des industriellen Produktionsprozesses auf und verändert die Fertigung in immer mehr Branchen. Unter den zehn größten Anmeldern von internationalen Patentfamilien im Bereich der additiven Fertigung (2001–2020) befanden sich zwei deutsche Unternehmen, Siemens und BASF, wie eine Studie des Europäischen Patentamts zeigte.⁹



⁹ Eine internationale Patentfamilie steht für eine bedeutende Erfindung, für die in zwei oder mehr Ländern weltweit Patentanmeldungen eingereicht wurden. Studie Innovationstrends in der Additiven Fertigung des Europäischen Patentamts (EPA): https://www.epo.org/en/service-support/publications?size=n_10_n&sort-field=lastname_lowercase&sort-direction=desc

In welchem Zusammenhang stehen 3D-Druck und geistiges Eigentum?

Da der 3D-Druck sowohl eine Fertigungs- als auch eine Digitaltechnik ist, erleichtert er das unerlaubte Kopieren von Objekten. Wie andere digitale Dateien sind auch CAD-Entwürfe einfach zu kopieren und schwer zu verfolgen. Das Kopieren wird auch durch die zunehmende Verfügbarkeit kostengünstiger 3D-Scanner, mit denen man ein handelsübliches Produkt einscannen, einen 3D-Entwurf erstellen und diesen online verbreiten kann, einer wachsenden Zahl von Personen möglich. 3D-Druck kann verschiedene Rechte des geistigen Eigentums verletzen.

Was sollten Sie als Nutzer eines 3D-Druckers beachten?

Das Urheberrecht schützt die Originalität eines Werks und das Recht des Schöpfers, es zu vervielfältigen – auch vor unbefugtem 3D-Druck. In ähnlicher Weise schützt das Designrecht die äußere Hülle und das ästhetische Erscheinungsbild eines Objekts – seine Form –, während ein Patent seine technische Funktion schützt.

Um Patent-, Urheberrechts- und Designrechtsverletzungen beim 3D-Druck zu vermeiden, ist es ratsam, sicherzustellen, dass Sie die erforderlichen Rechte oder Lizenzen für die von Ihnen verwendeten Modelle besitzen. Das gilt auch für entsprechende Designdateien auf Internetseiten, wie zum Beispiel Thingiverse, Cults, MyMiniFactory und Printables, die zwischenzeitlich Millionen Nutzer verzeichnen.

Denn Verletzungen können vorkommen:

- 1) Im Zusammenhang mit dem Erstellungsprozess eines
 - 3D-Modells und
 - der 3D-Replik.
- 2) Bei der Weitergabe (auch dem Hochladen) und der Nutzung eines
 - 3D-Modells und
 - der 3D-Replik.

Sofern Sie selbst gewerbliche Schutzrechte besitzen (Designs, Patente) oder auch urheberrechtlichen Schutz beanspruchen können, sollten Sie regelmäßig überprüfen, ob 3D-Repliken Ihres eigenen Produkts auf entsprechenden Webseiten angeboten werden. Wenn ja: Ergreifen Sie entsprechende Maßnahmen, um Ihre CAD-Dateien vor unautorisiertem Zugriff und Weiterverbreitung zu schützen.



QR-Code zur Broschüre
„Rechte an geistigem
Eigentum durchsetzen“

Rechte des geistigen Eigentums in Deutschland im Zusammenhang mit 3D-Druck

Recht des geistigen Eigentums	Was ist geschützt?	Was ist nicht geschützt?
Urheberrecht	<ul style="list-style-type: none"> • Eine <u>CAD-Datei</u>, die von Grund auf erstellt wurde. • Computergestützte Rekonstruktionen. 	<ul style="list-style-type: none"> • Werke, bei denen die Schutzfrist bereits abgelaufen ist. • Besondere Materialien für die Herstellung. • Gestaltungsmerkmale, die technisch zwingend oder zumindest sehr weitgehend technisch bedingt sind.
Designrecht	<ul style="list-style-type: none"> • Die äußere Form und Merkmale des gesamten oder eines Teils des Erzeugnisses. • Das Erscheinungsbild der Werkstoffe. • Eine <u>CAD-Datei</u> des Erzeugnisses. 	<ul style="list-style-type: none"> • Rohmaterialien. • Innere Teile, die bei normalem Gebrauch nicht sichtbar werden. • Ein Gegenstand, der alltäglich ist, in dem betreffenden technischen Bereich. • Werkstücke, die für mechanische Verbindungen mit einem anderen Produkt konstruiert sind (beispielsweise bestimmte Schrauben und Muttern). • Merkmale, die durch die technische Funktion des Objekts bestimmt sind. • Nach § 40a Designgesetz (DesignG) „besteht kein Designschutz für ein Design, das als Bauelement eines komplexen Erzeugnisses mit dem Ziel verwendet wird, die Reparatur dieses komplexen Erzeugnisses zu ermöglichen, um diesem wieder sein ursprüngliches Erscheinungsbild zu verleihen (insbesondere Karosserieersatzteile).“
Patentrecht/ Gebrauchsmusterrecht	<ul style="list-style-type: none"> • Die Innovation und Technologie, die dem Objekt innenwohnt. • Eine <u>CAD-Datei</u>, die einen Plan für den patentierten Gegenstand enthält, wenn er in den Patentansprüchen zitiert wird. • Ein Bauteil oder Produkt, das als solches durch ein Patent oder Gebrauchsmuster geschützt ist, darf weder mithilfe des 3D-Drucks gewerblich hergestellt werden noch mittels anderer Herstellungsverfahren. Auch dann nicht, wenn es dringend als Ersatzteil benötigt wird. • Hat das mit dem 3D-Drucker erstellte Ersatzteil einen engen Bezug zu einem wesentlichen Element der patentierten Erfindung, ist seine Herstellung und sein Vertrieb als mittelbare Patentverletzung gem. § 10 Patentgesetz (PatG) oder als mittelbare Gebrauchsmusterverletzung zu bewerten und daher verboten. 	<ul style="list-style-type: none"> • Ästhetische Gestaltung.

Was gilt bei 3D-Druck durch Privatpersonen?

- Für **Design, Marke und Patent** gilt: Eine Nachbildung mithilfe des 3D-Drucks ist erlaubt, sofern diese im privaten Bereich zur nichtgewerblichen Nutzung stattfindet. Der private Gebrauch dient ausschließlich der Befriedigung persönlicher Bedürfnisse wie Bildung oder Unterhaltung und jener von engen Freunden, Bekannten und Verwandten. Juristische Personen können keinen privaten Gebrauch geltend machen.
- Bei **urheberrechtlich geschützten Werken** ist die Anfertigung einzelner 3D-Repliken zum Privatgebrauch (also insbesondere nicht zu Erwerbszwecken) ebenfalls erlaubt. Darüber hinaus ist zu beachten, dass zur Vervielfältigung keine offensichtlich rechtswidrig hergestellte oder offensichtlich rechtswidrig ins Internet gestellte Vorlage verwendet werden darf, etwa eine „raubkopierte“ CAD-Datei. Die 3D-Replik darf nicht weiterverbreitet – insbesondere nicht verkauft – oder öffentlich wiedergegeben werden, zum Beispiel im Rahmen einer Ausstellung.

Möglicher präventiver Schutz:

- Digital Rights Management für Softwaredateien mit Anweisungen zum 3D-Druck des Objekts.
- Geheimhaltung bestimmter Informationen, wie beispielsweise der Rohmaterialien für die Zusammensetzung eines Objekts oder bestimmter Herstellungsverfahren und -methoden.
- Aufbau von Strategien für das Kundenbeziehungsmanagement (Customer Relationship Management, CRM), zum Beispiel für die Lieferung von authentischen, autorisierten CAD-Dateien und Rohmaterialien, die für den 3D-Druck benötigt werden.

Rechte durchsetzen im digitalen Raum

110010

Rechtsverletzungen finden – Monitoring.

Software kann Ihnen das Monitoring erleichtern, zum Beispiel, indem die Anwendung Internetseiten oder Social Media nach Inhalten scannt, die Ihre geistigen Eigentumsrechte verletzen könnten. Einige Anwendungen bieten auch automatisierte Unterstützung bei der Entfernung solcher Inhalte an, sogenannter Takedown.

Das Monitoring hilft nicht nur bei der Suche nach möglichen Produktfälschungen, sondern auch beim Aufspüren von unerlaubten Verwendungen Ihrer Fotos, zum Beispiel Ihrer Werbefotos.

Bei der Aufdeckung von Produktfälschungen spielt auch der Einsatz Künstlicher Intelligenz eine zunehmend wichtige Rolle: Zum Beispiel durch die systematische Analyse von Zertifikaten, Zolldaten und Handelsregistereinträgen kann KI Unstimmigkeiten aufdecken und so Hinweise auf gefälschte Produkte und die Netzwerke dahinter liefern. Auch die Auswertung von Handels- und Transportdaten kann es ermöglichen, illegale Aktivitäten frühzeitig zu erkennen, wie etwa den Vertrieb gefälschter Produkte über bekannte Schmuggelrouten.

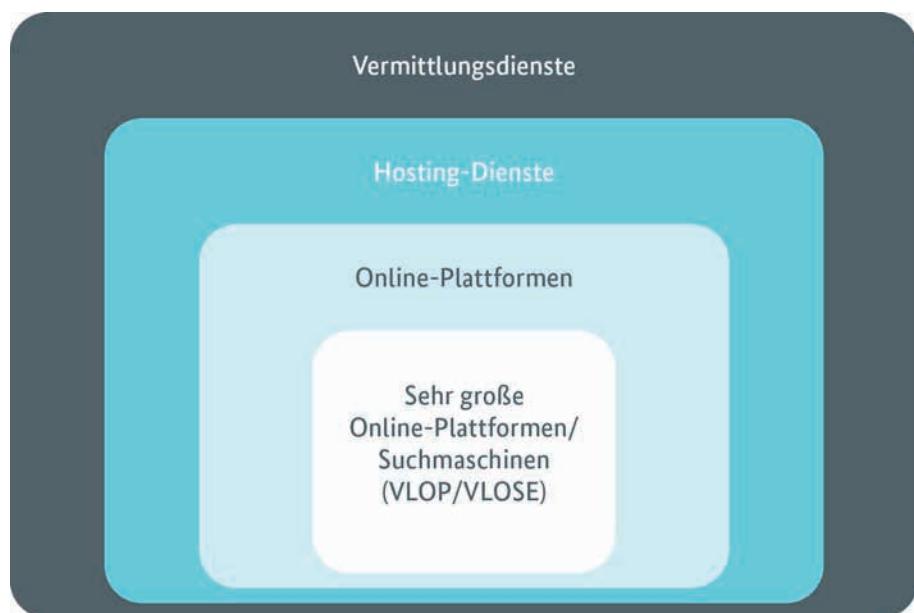
Illegale Inhalte online melden – diese Regelungen des Digital Services Act (DSA) sollten Sie kennen.

Wie bei anderen Rechtsverletzungen im digitalen Raum auch, ist Schnelligkeit bei der Durchsetzung von Rechten des geistigen Eigentums ein ganz wesentlicher Faktor. Nur so kann die Weiterverbreitung illegaler Inhalten wirksam eingegrenzt werden. Bei Online-Inhalten ist eine Vielzahl von Akteuren beteiligt. Besonders wichtig sind die Anbieter sogenannter Vermittlungsdienste. Voraussetzung für eine effektive Rechtsdurchsetzung sind daher klare Regeln: Wer ist für die Prüfung rechtswidriger Inhalte zuständig? Und wie kann ich auf Rechtsverletzungen aufmerksam machen? Hierfür wurde auf EU-Ebene der Digital Services Act verabschiedet.

Um die Anbieter dieser Dienste geht es im DSA insbesondere:

- **Vermittlungsdienst:** Ein großer Sammelbegriff für alle, die Internet-Infrastruktur zur Verfügung stellen, zum Beispiel WLAN-Dienste oder Domain-Registrierungsstellen, aber auch Cloud-Dienste oder Social-Media-Plattformen.
- **Hosting-Dienst:** Ein Unterfall des Vermittlungsdienstes: Er speichert vom Nutzer bereitgestellte Informationen in dessen Auftrag, zum Beispiel Web-hosting- und Cloud-Dienste.

- **Online-Plattformen:** Ein Unterfall eines Hosting-Dienstes, der nicht nur die vom Nutzern bereitgestellten Informationen speichert, sondern diese auch öffentlich verbreitet. Online-Plattformen begegnen uns im Alltag etwa in Form von E-Commerce-Plattformen, aber auch als Social-Media-Plattformen.
- **Sehr große Online-Plattformen und Suchmaschinen:** Sie werden monatlich von mindestens 45 Millionen Nutzerinnen und Nutzern in der Union besucht.



Was ist der DSA?



QR-Code zur Broschüre „Rechte an geistigem Eigentum durchsetzen“

Stellen Sie sich vor, Sie finden im Rahmen des Monitorings auf einer E-Commerce-Plattform einen Händler, der Ihr geschütztes Markenzeichen missbräuchlich verwendet. Wie Sie gegen den Händler vorgehen können, haben wir in unserer Broschüre „Rechte an geistigem Eigentum durchsetzen“ gezeigt. Ein anderer Weg ist, diese rechtsverletzenden Inhalte der Plattform zu melden, damit diese die Inhalte prüft und das markenverletzende Angebot nicht mehr zugänglich macht. Dieses Melde- und Abhilfeverfahren, aber auch einige weitere wichtige Regelungen, sind im Digital Services Act enthalten.

Der Digital Services Act ist eine EU-Verordnung. Als EU-Verordnung gilt der DSA unmittelbar: komplettiert wird er durch das Digitale Dienste Gesetz. Der DSA soll – kurz gesagt – zu einem sichereren und vertrauenswürdigeren Internet beitragen. Insbesondere, indem dort weniger illegale Inhalte auffindbar sind.

Dabei können illegale Inhalte verschiedene Bereiche betreffen: zum Beispiel Hate Speech, also strafrechtlich relevante beleidigende oder bedrohende Äußerungen, terroristische Inhalte, illegaler Verkauf von Tieren – oder eben die Verletzung Ihres geistigen Eigentums. Der DSA gilt für alle Vermittlungsdienste, die Nutzerinnen und Nutzern in der EU angeboten werden – egal, ob diese Anbieter selbst einen Sitz in der EU haben oder nicht. Zusätzliche Konkretisierungen erhält der DSA durch das deutsche Digitale-Dienste-Gesetz.

Warum ist der DSA so wichtig zum Schutz von geistigen Eigentums?

Der DSA erlegt Anbieterinnen und Anbietern von Vermittlungsdiensten verschiedene Pflichten auf. Hierzu gehören insbesondere:

- **Melde- und Abhilfeverfahren („notice and action“):** Anbieter von Hosting-Diensten – also Dienste, die Inhalte speichern – müssen Meldesysteme einrichten und auf gemeldete illegale Inhalte reagieren. Zum Beispiel durch Entfernen des Inhalts oder Sperrung des betreffenden Accounts. Wenn Sie das Meldesystem in Anspruch nehmen, müssen Sie verschiedene Informationen angeben. Insbesondere, warum aus Ihrer Sicht ein illegaler Inhalt vorliegt. Die Eintragung einer Marke oder von Designs kann sehr hilfreich sein, um eine Verletzung Ihrer Rechte nachzuweisen.
- **Trusted Flagger:** Meldungen im Rahmen des „notice and action“-Verfahrens können bei Online-Plattformen zum Beispiel von Nutzerinnen und Nutzern, aber auch von sogenannten **Trusted Flaggern** gemacht werden. Das sind vertrauenswürdige Hinweisgeber. Ihre Meldungen werden von den Diensteanbietern prioritätär behandelt. Eine Liste aller akkreditierten europäischen Hinweisgeber finden Sie hier:  <https://digital-strategy.ec.europa.eu/de/policies/trusted-flaggers-under-dsa>
- **Pflichtangaben zu Unternehmen:** Online-Plattformen, bei denen Unternehmen mit Verbraucherinnen und Verbrauchern Verträge abschließen können, müssen sicherstellen, dass diese Unternehmen vor Nutzung der Plattform bestimmte Angaben machen: etwa zu Kontaktmöglichkeiten und Anschrift. Dies kann helfen, im Verletzungsfall Ansprüche leichter durchzusetzen.



Nicht alle Regeln gelten für alle Arten von Diensten. Eine Faustregel: Je größer die Rolle des Dienstes in Bezug auf den illegalen Inhalt ist, desto mehr Regeln muss er beachten. Deshalb gelten für Dienste, die einen Inhalt lediglich speichern, weniger Regeln als für große Online-Marktplätze, auf deren Inhalte monatlich viele Millionen Nutzerinnen und Nutzer zugreifen. Kleine Anbieter, die weniger als 50 Personen beschäftigen und deren Jahresumsatz oder Jahresbilanzsumme 10 Mio. Euro nicht übersteigt, sind übrigens von vielen Pflichten ausgenommen.

Was passiert, wenn ein Dienst die Pflichten nicht umsetzt?

Das regeln der DSA sowie das Digitale-Dienste-Gesetz:

- Wenn der Anbieter eines Hosting-Dienstes gemeldete Inhalte nicht (rechtzeitig) löscht, kann sein Haftungsprivileg entfallen. Eine zivilrechtliche Haftung ist möglich, wenn durch die gemeldeten Informationen dem Dienstanbieter ohne eingehende rechtliche Prüfung die Feststellung möglich wäre, dass die einschlägige Tätigkeit oder Information rechtswidrig ist.
- Wenn ein Dienst seine Pflichten nicht erfüllt, können Sie sich an den Digital Services Coordinator (in Deutschland die Bundesnetzagentur) wenden. Dieser kann zwar selbst keine Inhalte entfernen, sammelt aber Verstöße und kann bei systematischen Verstößen sogar Zwangs- und Bußgelder verhängen.

Betreffen die Verstöße sehr große Plattformen, wird die EU-Kommission zuständig. Diese kann Buß- oder Zwangsgeldverfahren einleiten.

Weitere Informationen rund um den DSA erhalten Sie auf den Internetseiten der Bundesnetzagentur sowie der EU-Kommission:

 <https://www.dsc.bund.de/DSC/DE/3Verbraucher/2VB/start.html>



 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_de#wie-geht-es-weiter



Informationen sammeln mit WHOIS-Abfragen.

Was ist eigentlich eine WHOIS-Abfrage?

Wenn eine Domain Ihre Rechte verletzt, etwa, weil der Domainname Ihr Zeichen wiedergibt, kommt eine WHOIS-Abfrage bei DENIC in Betracht. Die DENIC ist die Registrierungsstelle für alle Domains mit dem Kürzel „.de“, zum Beispiel: dpma.de. Die Domain ist mit einer IP-Adresse verknüpft und sorgt dafür, dass Sie zum Aufruf einer Internetseite nicht umständlich eine lange Zahlenkombination (IP-Adresse) eingeben müssen. Mit einer WHOIS-Abfrage können Sie Informationen zu einer bestimmten Domain erlangen, insbesondere technische Daten zum Nameserver. Eine Auskunft über die Identität des Inhabers oder der Inhaberin einer Domain ist im Falle der nachweislichen Verletzung geistigen Eigentums grundsätzlich möglich. Die durch die Abfrage erhaltenen Informationen können ein erster Schritt bei der Durchsetzung Ihrer Rechte sein.

Weitere Informationen finden Sie unter:

💻 <https://www.denic.de/fragen-antworten>



Das DPMA als digitaler Dienstleister.

Die kostenfreie Recherche in den elektronischen Datenbanken **DEPATISnet** und **DPMAregister** ist vom heimischen Rechner oder unterwegs jederzeit möglich. Patente, Gebrauchsmuster, Marken und Designs: Die Datenbank **DPMAregister** dient quasi als „digitales Grundbuch“ der deutschen gewerblichen Schutzrechte. Wer ist Anmelder oder Inhaberin? Ist das Schutzrecht noch in Kraft? Wie ist der aktuelle Verfahrensstand? In **DPMAregister** finden Sie die Antworten!

Über **DEPATISnet** können Sie auf das Dokumentenarchiv zugreifen, das auch die Patentprüferinnen und Patentprüfer des DPMA für ihre Arbeit nutzen. Rund 160 Millionen Patentveröffentlichungen aus aller Welt sind in dieser Datenbank enthalten, und es werden stetig mehr. Das Eintauchen in diese Informationen kann Ihnen auch als Inspiration für neue Lösungen dienen!

Digital können auch die meisten Schutzrechtsanmeldungen vorgenommen werden: Von der Einreichung einer Patentanmeldung bis zur Anmeldung von Marken, Designs oder Gebrauchsmustern und anderen Schutzrechten sind Verfahren elektronisch möglich, und werden zudem mit Nachlässen bei den Anmeldegebühren honoriert. So ist über **DPMAdirektWeb** beispielsweise eine einfache Design- oder Markenanmeldung online ohne Signaturkarte oder spezielle Software in kurzer Zeit realisierbar. Mittlerweile sind auch digitale Nachreicherungen zu bereits laufenden Anmeldeverfahren möglich.

Bei der Bearbeitung von Patentanmeldungen kommen standardmäßig KI-Systeme für die Klassifizierung und für die Übersetzung von fremdsprachigen Quellen zum Einsatz.

Die Akten zu den registrierten Schutzrechten werden durchgängig in elektronischen Datenbanken geführt, der Austausch der Schutzrechtsinformationen zwischen den Ämtern geschieht ebenfalls digital.

Glossar.

C M B Z C G Z J G X H A I C Z
P F F Y Z R C J H C I B S L T Z
G T Z H K N Y Q E O A S L H N
A I A A B L Y F M D N Y S M B P
G D T Z N E N K H R D Q O P R
D D B G N T
Q J Q C E
U B Q W J
D Q H V R
O V M O U E G L S U A F H V Q M
W X T V Y L P L A K W F B Q Z
X Z O K Y Z S M V D H J I W T C
Z U X Y Y S L L M Z F N G D W
K E P Z U O B A D G G T X C R Y
V H z U I A o S J F Q U U M T
D M o o K N K F H T Q O K S I E
P X s A T E M W Q o s a b x e
H Q U Y Z O B A Y Q H W A M E Z
H M M Y K A J K R L Q V L O A
N D W G Q Y O X W M K I k q y
G Y Z X U Z D G O U W T s t d
T Y H B K T A L C O Q X d s m e
I K M N Q N I S H I E B X K S A
C A I A Z K W G U B P N D N I C
S J V F L U J T E F P T T U L K
L J T x A X A Z R M C H Y A U Z
U C A F I Y J J I C B A C K K
R Z R z U K H O G U T Y O X G I
E Y G O L Q C H W L U L S J P
E W C M T E R R G W B M Z E X T
B Y J H I G G O V B L C M V O
P A R J R Y C U L Q M J A z v i
c Y U A R R Z U L N X G I M S
E D Y E V H L Q X T X H G E N I
G S Z R K A A M S K V T U Y H
E M I H I L S K L X J Y X D I L
X J Y T H P v x P E K E N N P

1, 2, 3

3D-Druck

Der 3D-Druck ist ein Oberbegriff, der mehrere Arten von Technologien umfasst, mit deren Hilfe sich ausgehend von einer digitalen Datei mittels eines 3D-Druckers körperliche Gegenstände herstellen lassen.

3D-Modell

Ein dreidimensionales Modell, das mit geeigneter Software erstellt oder modifiziert wurde, um den allgemeinen Anforderungen des 3D-Drucks gerecht zu werden. Ein solcher Entwurf kann auf der Grundlage eines bestehenden Produkts, einer Zeichnung, eines Bildes oder einer Skizze erstellt werden. Eine OBJ-Datei ist ein weit verbreitetes Dateiformat in der 3D-Grafik und Computergrafik. Sie wird hauptsächlich verwendet, um 3D-Modelle von geometrischen Formen, Oberflächen und Texturen zu speichern.

↗ 3D-Druck

3D-Replik

Mit einer 3D-Replik eines Objekts wird versucht, die komplette Geometrie eines Objekts, seine Oberflächentextur und nach Möglichkeit seine optischen Materialeigenschaften zu erfassen und zu einem integrierten, digitalen 3D-Modell zusammenzuführen, welches das Original möglichst originalgetreu abbildet.

A

Avatar

Grafische Darstellung, Animation, Karikatur oder Ähnliches als Verkörperung des Benutzers im Metaverse.

↗ Metaverse

B

Blockchain

Eine spezielle Technologie, mit der Daten manipulations-sicher gespeichert werden können. Bekannte Anwendungsfälle sind Kryptowährungen wie der „Bitcoin“ und sogenannte NFT.

↗ NFT

C

CAD

Computer Aided Design - Oberbegriff für alle Entwurfsarbeiten, die mittels Computer vorgenommen und digital gespeichert werden.

CAD-Datei

Eine CAD-Datei ist das digitale Arbeitsergebnis, das von computergestützten Konstruktionsprogrammen zur Speicherung relevanter Zeichnungsinformationen erstellt wird. In einer CAD-Datei werden Bild- (2D oder 3D), Geometrie- und Metadaten (Daten über Daten) gespeichert.

↗ CAD

Computerimplementierte Erfindungen

Computerimplementierte Erfindungen, auch programmbezogene Erfindungen genannt, sind Erfindungen, zu deren Ausführung ein Computer, ein Computernetzwerk oder eine sonstige programmierbare Vorrichtung eingesetzt wird. Sie weisen mindestens ein Merkmal auf, das (zumindest teilweise) durch ein Computerprogramm, also durch Software, realisiert wird. In der Alltagssprache werden daher solche Erfindungen oft verkürzt als ‚Software‘-Erfindungen oder -Patente bezeichnet.

Creative Commons Lizenzen

Beispiel für Open-Content-Lizenz. Die amerikanische Stiftung Creative Commons hat verschiedene Standard-Lizenzen für offene Inhalte entwickelt. Die Verwendung der Lizenzen ist gratis.

↗ Open-Content-Lizenz

Cyberangriff

Eine „Einwirkung auf ein oder mehrere andere informatio-nstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informa-tions-technische Mittel ganz oder teilweise zu beeinträchtigen (gemäß Cyber-Sicherheitsstrategie der Bundesregierung für Deutschland 2016).

Cybersquatting

Dritte registrieren böswillig Domännamen zum Beispiel mit einem fremden Markennamen, ohne Erlaubnis der Markeninhaberin oder des Markeninhabers.

D

Datenbank

Systematische Sammlung von Werken oder Daten, auf die einzeln zugegriffen werden kann. Datenbanken können durch Urheberrecht und verwandte Schutzrechte geschützt sein.

Design

Ein Design ist (noch) definiert als „zweidimensionale oder dreidimensionale Erscheinungsform eines ganzen Erzeug-nisses oder eines Teils davon“. Es ergibt sich zum Beispiel aus den Linien, Konturen, Farben, der Gestalt, Oberflächen-struktur beziehungsweise den Werkstoffen des Erzeugnisses. Mit der Umsetzung der EU-Designnovelle wird der Designbegriff auf unkörperliche, beispielsweise animierte und virtuelle Designs, erweitert werden.

Digitale-Dienste-Gesetz (DDG)

Deutsches Gesetz, das die Umsetzung des DSA in Deutsch-land regelt. Zum Beispiel, wer zuständig ist und wie hoch die Bußgelder für Verstöße gegen Pflichten aus dem DSA sein können.

↗ DSA

Digital-Rights-Management (DRM)

Schutz geistigen Eigentums mithilfe von Technik.

Domain

Eine Domain ist das, was Sie in Ihre Browserleiste tippen (zum Beispiel: www.dpma.de). Sie besteht aus einer Third-Level-Domain (etwa www), einer Second-Level-Domain (dpma) und einer Top-Level-Domain (de). Die Domain ist mit einer IP-Adresse verknüpft und sorgt dafür, dass Sie zum Aufruf einer Internetseite nicht umständlich eine lange Zahlenkombination (IP-Adresse) eingeben müssen. Domains müssen registriert werden. Für die Verwaltung des Registers mit allen .de-Domains ist die DENIC zuständig.

DSA (Digital Services Act)

Der Digital Services Act ist eine EU-Verordnung. Der DSA gilt unmittelbar in Deutschland, da er eine EU-Verordnung ist und wird durch das Digitale-Dienste-Gesetz komplettiert. Der DSA soll - kurz gesagt - zu einem sicheren und ver-trauenswürdigen Internet beitragen. Insbesondere, indem dort weniger illegale Inhalte auffindbar sind.

DSC (Digital Services Coordinator)

Zentrale Kontaktstellen für den DSA, in Deutschland die Bundesnetzagentur.

↗ DSA

F

Fake Shop

Ein Betrugsmodell mithilfe eines Online-Shops, der oft den Webauftritt bekannter Markeninhaber kopiert. Verbraucher bezahlen für Ware, die sie aber niemals erhalten.

G

General purpose AI-Modell

deutsch: KI-Modell mit allgemeinem Verwendungszweck; kann verschiedenen Zwecken dienen (sowohl direkte Ver-wendung als auch Integration in andere KI-Systeme mög-lich). Begriff aus der KI-Verordnung.

↗ KI-Verordnung

↗ Generative KI

Generative KI

Eine generative KI erlernt Muster und Strukturen anhand von Trainingsdaten und generiert daraus auf Anforderung neue Daten mit ähnlichen Strukturen und Eigenschaften.

Geschäftsgeheimnis

Eine Information, die nicht allgemein bekannt und daher von wirtschaftlichem Wert ist, durch angemessene Geheimhaltungsmaßnahmen geschützt ist und an deren Geheimhaltung ein berechtigtes Interesse besteht.

H

Hate Speech

deutsch: Hass-Rede. Soweit diese rechtswidrig ist, etwa weil sie strafrechtlich relevant ist, finden die Regelungen des DSA Anwendung.

Hosting-Dienst

Ein Unterfall des Vermittlungsdienstes: Er speichert vom Nutzer bereitgestellte Informationen in dessen Auftrag (zum Beispiel Webhosting und Cloud-Dienste). Durch den DSA müssen die Dienste verschiedene Regeln beachten.

- ↗ DSA
- ↗ Vermittlungsdienst
- ↗ Online-Plattform

K

KI-Verordnung

Europäische Verordnung, die den Zweck verfolgt, den Einsatz Künstlicher Intelligenz zu fördern und zugleich ein hohes Schutzniveau für wichtige Güter wie Gesundheit und Sicherheit zu gewährleisten.

Künstliche Intelligenz (KI)

Mit „Künstlicher Intelligenz“ werden alle Computerprogramme mit hinterlegten Datenbanken bezeichnet, die in der Lage sind, aufgrund der Eingaben von Nutzern mit sinnvollen Ausgaben zu reagieren.

L

Leistungsschutzrecht

Der Verwandte des Urheberrechts. Leistungsschutzrechte gibt es zum Beispiel für Fotos, die nicht originell genug sind, um ein Werk zu sein (Schnappschüsse, Selfies). Oder für Personen, die zwar keine Urheberin oder kein Urheber sind, aber am Werk (künstlerisch oder finanziell) mitgewirkt haben (etwa Musikerinnen und Musiker, Herstellerinnen von Datenbanken oder Filmen). Auch diese Inhalte sind geschützt, haben aber einige Besonderheiten (zum Beispiel kürzere Schutzdauer).

Lizenz

Ein Vertrag, der regelt, wie ein Recht des geistigen Eigentums genutzt werden darf. Es gibt ausschließliche Lizenzen, die nur einer Person Nutzungsrechte geben. Einfache Lizenzen ermöglichen mehreren Leuten die Nutzung. Man kann Lizenzen auch nur für bestimmte Nutzungen erteilen.

Locarno-Klassifikation

Eine Liste, die international Produktbereiche bzw. Erzeugnisse in insgesamt 32 Hauptklassen und 241 Unterklassen einteilt. Durch die Klassifikation sind eingetragene Designs leichter recherchierbar. Die Erzeugnisangabe ist wichtiger Bestandteil einer Designanmeldung.

M

Malware

Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen.

Melde- und Abhilfeverfahren

Englisch „notice and action“. Regelung des DSA, wonach Hosting-Dienste verpflichtet sind, ein Meldesystem für illegale Inhalte anzubieten. Sie müssen eingegangene Meldungen bearbeiten und auf hierdurch erkennbare illegale Inhalte reagieren.

- ↗ DSA
- ↗ Notice and Action
- ↗ Hosting-Dienst

Meme

Foto oder Video, das mithilfe von Text in einen unerwarteten und dadurch humorvollen oder ironischen Kontext gesetzt wird. Wichtiges Ausdrucksmittel in der Internetkultur/Social Media.

Metaverse

Vielzahl digitaler Welten, in denen Avatare virtuell zusammenkommen und miteinander interagieren können. Besonders realistische Darstellungen werden durch VR- bzw. AR-Brillen ermöglicht, mit denen man entweder vollständig in eine virtuelle Welt eintaucht (VR: virtual reality) oder in die reale und virtuelle Welt miteinander verschmelzen (AR: augmented reality). Inzwischen sind Metaversen auch ohne Hilfsmittel erlebbar.

Monitoring

Systematische Beobachtung des Internets auf Verletzungen des eigenen geistigen Eigentums.

N

NFT

Englisch: Non-fungible Token, Deutsch: nicht-austauschbare Wertmarke: Eine Art digitales Zertifikat, durch das man unter anderem nachweisen kann, Besitzerin oder Besitzer einer Originaldatei zu sein, zum Beispiel einer Fotografie. NFT werden in der Blockchain gespeichert und sind daher manipulationssicher.

↗ Blockchain

Nizza-Klassifikation

Eine Liste, die international 45 Klassen (34 für Waren, 11 für Dienstleistungen) festlegt. Das Waren- und Dienstleistungsverzeichnis ist wichtiger Bestandteil einer Markenanmeldung.

Notice and Action

deutsch: Melde- und Abhilfeverfahren

↗ Melde- und Abhilfeverfahren

O

Online-Plattform

Online-Plattformen begegnen uns im Alltag in Form von App-Stores oder Online-Marktplätzen, aber auch als Social-Media-Plattformen: Es werden nicht nur Inhalte gespeichert, sondern die Inhalte sind auch öffentlich einsehbar, zum Beispiel angebotene Ware auf einer E-Commerce-Plattform. Unterfall des Vermittlungsdienstes und des Hosting-Dienstes. Online-Plattformen müssen im DSA mehr Regeln beachten, als zum Beispiel reine Hosting-Dienste.

- ↗ DSA
- ↗ Hosting-Dienst
- ↗ Vermittlungsdienst

Open Content

Deutsch: „offene Inhalte“. Werke sind grundsätzlich urheberrechtlich geschützt. Möchte man diese der Öffentlichkeit frei zugänglich machen, kann man diese als „offene Inhalte“ kenntlich machen. Hierbei helfen Open-Content-Lizenzen. Nutzerinnen und Nutzer können dann das Werk gratis verwenden, wenn sie die Regeln der Lizenz einhalten.

↗ Open-Content-Lizenz

Open-Content-Lizenz

Deutsch: Lizenz für „offene Inhalte“. Lizenzen sind Regeln, nach denen die Nutzung eines Rechts, zum Beispiel an einem Werk, erlaubt ist. Open-Content-Lizenzen legen also die Regeln fest, die man beachten muss, wenn man ein unter dieser Lizenz veröffentlichtes Werk verwenden möchte. Zum Beispiel: Keine Bearbeitung oder keine kommerzielle Nutzung.

↗ Lizenz

Opt-Out

Nutzungsvorbehalt; ein wirksamer Nutzungsvorbehalt kann Text und Data Mining zu kommerziellen Zwecken untersagen.

↗ Text und Data Mining

Output

Englisch: Ausgabe. Inhalte, die von einer Künstlichen Intelligenz ausgegeben/erzeugt werden.

↗ KI

P

Phishing

Phishing setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing erhält der Adressat eine vermeintlich authentische E-Mail. Der E-Mail ist häufig ein Dokument als Anhang beigelegt oder sie enthält Verlinkungen auf andere Webseiten, die beim Öffnen in der Regel dazu führen, dass Passwörter und Zugangsdaten unrechtmäßig ausgespäht werden.

T

Technizität

Technizität bezeichnet die Eigenschaft einer Erfindung, auf einem technischen Gebiet zu liegen, wie in § 1 Abs. 1 Patentgesetz (PatG) festgelegt.

Text und Data Mining

Automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen.

Tracking

Englisch: Verfolgung. Besonders relevant ist die Nachverfolgung von Inhalten im Internet.

Trusted Flaggers

Englisch: vertrauenswürdige Hinweisgeber sind besondere Einrichtungen im Rahmen des DSA. Sie müssen durch die Bundesnetzagentur zertifiziert werden. Wenn sie illegale Inhalte melden, müssen Online-Plattformen diese Meldungen prioritär behandeln.

↗ DSA

V

Vermittlungsdienst

Ein großer Sammelbegriff für alle Dienste, die Internet-Infrastruktur zur Verfügung stellen, zum Beispiel Internetzugangsanbieter oder Domain-Registrierungsstellen, aber auch Cloud-Dienste oder Social-Media-Plattformen. Durch den DSA müssen die Dienste verschiedene Regeln beachten.

↗ DSA

W

WHOIS-Abfrage

Eine Abfrage, mit der man den Inhaber oder die Inhaberin einer Domain sowie weitere technische Informationen (zum Beispiel den Nameserver) herausfinden kann.

↗ Domain

Wir schützen nicht nur Innovationen.

Impressum

Herausgeber
Deutsches Patent- und Markenamt
Zweibrückenstraße 12
80331 München

Telefon +49 89 2195-1000
www.dpma.de

Stand
Oktober 2025

Bildnachweis
via Getty Images:
Titel: piranka, Seite 5: TIM VERNON/SCIENCE PHOTO LIBRARY, Seite 8: Flavio Coelho, Seite 9: Pikusisi-Studio, Seite 10: Aleksandra Konoplia, Seite 12: We Are, Seite 13: da-kuk, Seite 15: We Are, Seite 18: sankai, Seite 21: Sandipkumar Patel, Seite 24: Curly_photo, Seite 25: teekid, Seite 26: WLADIMIR BULGAR/SCIENCE PHOTO LIBRARY, Seite 30: mattjeacock, Seite 35: D3Damon, Seite 37: olaser

iStock.com:
Seite 17: Urupong

Diese Informationsbroschüre soll einen ersten Überblick vermitteln über geistiges Eigentum in der digitalen Welt. Die Broschüre enthält daher auch vereinfachte und verallgemeinernde Aussagen. Eine vollständige und verbindliche Darstellung der komplexen Materie ist in diesem Rahmen nicht möglich. Weitergehende Informationen erhalten Sie auch auf den Internetseiten des Deutschen Patent- und Markenamts: dpma.de

