

Der Prüfungsausschuss

Empfehlung zur Umsetzung einer DNS-Sperre

Auf Antrag von

Antragstellerin

hat der Prüfungsausschuss durch

als Vorsitzenden

als Beisitzer

aufgrund der Beratung in der Sitzung vom 22. Juli 2024 einstimmig beschlossen:

Es wird empfohlen, für die Website

GetRockMusic

verfügbar unter

eine DNS-Sperre umzusetzen.

Begründung:

1. Tätigkeit des Prüfungsausschusses

- I. Der Prüfungsausschuss wird tätig aufgrund Nr. 3 des Verhaltenskodexes i.V.m. §§ 6, 7 der Verfahrensordnung (Anl. 1 des Verhaltenskodexes).
- II. Die Empfehlung zur Sperrung der Website erfolgt ausschließlich aufgrund gesetzlicher Vorschriften. Sie erfolgt nur, wenn eine klare Verletzung des deutschen Urheberrechtsgesetzes festgestellt ist.

2. Zulässigkeit des Antrags

Der Prüfantrag ist zulässig.

Ein Prüfantrag ist nach § 7 Abs. 1 der Verfahrensordnung zulässig, wenn a) die Antragsberechtigung vorliegt und b) die Prüfungsgebühren vorab entrichtet sind.

Nach § 7 Abs. 3 Verfahrensordnung ist jeder Rechteinhaber antragsberechtigt, der Partei des Verhaltenskodexes ist, oder Mitglied eines Verbandes ist, der Partei des Verhaltenskodexes ist und der dem Antrag zugestimmt hat.

Diese Voraussetzungen sind erfüllt. Die Antragstellerin ist Mitglied des Verbands „Bundesverband Musikindustrie e. V. (BVMI)“, der Partei des Verhaltenskodexes ist und der dem Antrag zugestimmt hat (Anlage 1).

Die Prüfgebühren sind vorab entrichtet. Die Einzahlung ist belegt (Anlage I.2).

3. Begründetheit des Antrags

Der Antrag auf Empfehlung der Sperrung der Website GetRockMusic ist begründet. Die Website ist eine strukturell urheberrechtsverletzende Website (SUW). Es liegt eine klare Verletzung des Urheberrechts vor. Die Sperrung ist zumutbar und verhältnismäßig.

I. Antrag

Die Antragstellerin beantragt, für die strukturell urheberrechtsverletzende Website GetRockMusic eine DNS-Sperre gemäß dem Verhaltenskodex DNS-Sperren umzusetzen, unabhängig von dem durch die strukturell urheberrechtsverletzende Website gewählten http-Protokoll.

Bedenken hinsichtlich der Bestimmtheit des Antrags bestehen nicht.

II. Voraussetzungen der Empfehlung

Nach Art. 8 Abs. 3 der Richtlinie 2001/29/EG stellen die Mitgliedstaaten sicher, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. Art. 11 S. 3 der Richtlinie 2004/48/EG sieht vor, dass die Mitgliedstaaten unbeschadet des Art. 8 Abs. 3 der Richtlinie 2001/29/EG ferner sicherstellen, dass die Rechtsinhaber eine Anordnung gegen Mittelspersonen beantragen können, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden. Gemäß Art. 17 Abs. 2 der EU-Grundrechtecharta wird geistiges Eigentum geschützt.

Zum Teil wird die Auffassung vertreten, als Rechtsgrundlage für eine DNS-Sperre seien die Grundsätze der Störerhaftung heranzuziehen (LG München I, Urt. v. 01.02.2018 – 7 O 17752/17, CR 2018, 611 – kinox.to; für die Zeit vor Neufassung des § 7 Abs. 4 TMG durch das Dritte Gesetz zur Änderung des Telemediengesetzes vom 28.09.2017: BGH, Urt. v. 26.11.2015 – I ZR 174/14 GRUR 2016, 268 Rn. 20 ff. – Störerhaftung des Access-Providers) oder es wird angenommen, Art. 8 Abs. 3 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft könne als unmittelbare Anspruchsgrundlage dienen. Teilweise wurde auch § 7 Abs. 4 TMG direkt oder analog für einen gesetzlichen Anspruch gegen einen Zugangsanbieter zur Verhängung einer DNS-Sperre herangezogen (BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 18 und 19 – DNS-Sperre; OLG München, Urt. v. 17.10.2019 – 29 U 1661/19, MMR 2020, 35; betreffend sog. Tor-Exit-Nodes zum TOR-Netzwerk BGH, Urt. v. 26.07.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 42 – Dead Island). Das Telemediengesetz ist seit dem 14.05.2024 außer Kraft getreten (Art. 37 Abs. 2 des Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.06.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze, BGBl. I 2024 Nr. 149 vom 13.05.2024). An die Stelle des § 7 Abs. 4 TMG ist mit Wirkung vom 14.05.2024 § 8 des Digitale-Dienste-Gesetzes (DDG) über den Anspruch auf Sperrung bei Rechtsverletzung getreten (BGBl. I 2024 Nr. 149). Daneben sieht § 109 Abs. 3 Medienstaatsvertrag Maßnahmen gegen Diensteanbieter von fremden Inhalten vor. Die Voraussetzungen aller Rechtsgrundlagen sind weitgehend deckungsgleich.

Der Prüfungsausschuss lässt offen, ob eine DNS-Sperre gegen einen Zugangsvermittler nach den Maßstäben der Störerhaftung verhängt werden kann (zu den Grundsätzen BGH, Urt. v. 15.10.2020 – I ZR 13/19, NJW 2021, 311 Rn. 12 bis 35 – Störerhaftung des Registrars). Der Prüfungsausschuss hat auf der Grundlage der Rechtsprechung des Bundesgerichtshofs (BGH, Urt. v. 26.07.2018 – I ZR 64/17, GRUR 2018, 1044 Rn. 42 und 45 bis 49 – Dead Island; Urt. v. 15.10.2020 – I ZR 13/19, NJW 2021, 311 Rn. 27 – Störerhaftung des Registrars; Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 18 – 21 – DNS-Sperre) seiner Prüfung, ob die Voraussetzungen einer DNS-Sperre vorliegen, unter Geltung des Telemediengesetzes § 7 Abs. 4 TMG zugrunde gelegt. § 7 Abs. 4 TMG war nach der Rechtsprechung für den Sperranspruch gegen den Betreiber eines Internetzugangs direkt anwendbar, wenn der Zugang drahtlos vermittelt wurde; entsprechend war er anzuwenden, wenn der Sperranspruch gegen den Betreiber eines drahtgebundenen Zugangs gerichtet war (BGH, Urt. v. 26.07.2018 – I ZR 64/17, GRUR 2018, 1044, Rn. 49 – Dead Island; Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 21 – DNS-Sperre). Nachdem § 7 Abs. 4 TMG seit dem 14.05.2024 nicht mehr in Kraft ist, legt der Prüfungsausschuss seiner Empfehlung die Vorschrift des § 8 DDG zugrunde, die an die Stelle des § 7 Abs. 4 TMG getreten ist.

Die Vorschriften der Verordnung (EU) 2022/2065 über einen Binnenmarkt für digitale Dienste (Digital Services Act), die am 17.02.2024 in Kraft getreten sind, stehen einer nationalen Regelung, durch die die Vorgaben des Art. 8 Abs. 3 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft und des Art. 11 Satz 3 der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums umgesetzt werden, und damit § 8 DDG nicht entgegen (Begründung des Regierungsentwurfs vom 22.12.2023 zur Durchführung der Verordnung (EU) 2022/2065 (BR-Drucks. 676/23 S. 75)).

1. § 8 DDG

Der Antrag auf Empfehlung zur Umsetzung einer DNS-Sperre ist begründet, wenn die Voraussetzungen des § 8 DDG vorliegen. Wurde ein digitaler Dienst, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder den Zugang zu einem Kommunikationsnetz zu vermitteln, von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen, und besteht für den Inhaber des Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuwehren, so kann der Inhaber des Rechts nach § 8 Abs. 1 DDG von dem betroffenen Diensteanbieter die Sperrung der Nutzung von Informationen verlangen, um

die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein, § 8 Abs. 2 DDG.

Diensteanbieter im Sinne des § 8 DDG ist nach § 1 Abs. 4 Nr. 5 DDG ein Anbieter digitaler Dienste.

„Digitaler Dienst“ ist nach § 1 Abs. 4 Nr. 1 DDG ein Dienst i.S.d. Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft. Nach Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 ist „Dienst“ eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Darunter fällt ein Dienst, der Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellt oder einen drahtgebundenen Zugang zum Internet eröffnet. Auf die Bestimmung des Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 stellt auch Art. 3 lit. a der Verordnung (EU) 2022/2065 zur Definition des Dienstes der Informationsgesellschaft ab. Nach § 8 Abs. 4 Satz 1 DDG gelten § 8 Abs. 1 und 2 DDG auch dann, wenn der Dienst unentgeltlich erbracht wird. Danach sind Internetzugangsanbieter Anbieter digitaler Dienste und damit Diensteanbieter im Sinne von § 1 Abs. 4 Nr. 5 DDG.

2. Voraussetzungen für die Verhängung einer DNS-Sperre

Die Voraussetzungen für die Verhängung einer DNS-Sperre – und entsprechend die Grundsätze, die für die Empfehlung einer DNS-Sperre durch den Prüfungsausschuss mit Ausnahme der Einschränkung unter lit. c) gelten – sind danach:

- a) Der Anspruchsteller muss aktivlegitimiert sein,
- b) der Diensteanbieter muss Nutzern einen Zugang zum Internet vermitteln (diese Voraussetzung wird nachfolgend nicht weiter geprüft, weil alle Internetzugangsanbieter, die Partei des Verhaltenskodex sind, die Voraussetzung erfüllen),
- c) ein Diensteanbieter muss von einem Nutzer in Anspruch genommen werden, um das Recht am geistigen Eigentum eines anderen zu verletzen, wobei der Prüfungsausschuss eine Empfehlung zur DNS-Sperre nur dann ausspricht, wenn eine klare Rechtsverletzung vorliegt,
- d) für den Inhaber des Rechts darf keine andere Abhilfemöglichkeit bestehen und
- e) die Sperrung muss zumutbar und verhältnismäßig sein.

III. Vorliegen der Voraussetzungen

1. Aktivlegitimation des Anspruchstellers

Die Antragstellerin ist aktivlegitimiert. Sie ist Inhaberin von ausschließlichen Rechten am geistigen Eigentum. Die Antragstellerin ist Inhaberin von ausschließlichen Rechten an einem Leistungsschutzrecht des Tonträgerherstellers gem. §§ 15 Abs. 2 Nr. 2, 19a, 85 Abs. 1 Satz 1 UrhG im Hinblick auf das öffentliche Zugänglichmachen von Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download.

Der Antrag bezieht sich auf eine Verletzung der ausschließlichen Rechte der Antragstellerin an dem Tonträger „*****“ (nachfolgend Tonträger).

Die Leistungen des Tonträgerherstellers bestehen in der erstmaligen Aufnahme einer Darbietung oder Tonfolge auf einem Tonträger (Vogel in Schricke/Loewenheim, Urheberrecht, 6. Aufl., § 85 Rn. 24). Schutzgegenstand des Leistungsschutzrechts des Tonträgerherstellers ist keine künstlerische oder schöpferische Leistung, sondern das technische Können und die wirtschaftlichen Aufwendungen, die eine erstmalige Aufnahme einer Werkdarbietung oder einer Tonfolge auf einen Tonträger erfordern und damit die in dem Tonträger verkörperte wettbewerbliche Leistung (Boddien in Fromm/Nordemann, Urheberrecht, 12. Aufl., § 85 Rn. 1). Diese Leistung des Tonträgerherstellers ist auch in Deutschland geschützt.

Die Antragstellerin ist Rechtsinhaberin. Dies folgt gem. §§ 85 Abs. 4, 10 Abs. 1 UrhG aus der üblichen Bezeichnung der Antragstellerin als Tonträgerherstellerin auf den Vervielfältigungsstücken mit dem sog. P-Vermerk und der Jahreszahl (Boddien in Fromm/Nordemann, Urheberrecht, 12. Aufl., § 85 Rn. 71), die durch die Anlage II.1 belegt sind.

2. Strukturell urheberrechtsverletzende Website (SUW)

Die Website ist in englischer Sprache gehalten (Ermittlungsbericht ***** vom *****, Anlage II.2.5). Sie ist gleichwohl auf den deutschsprachigen Markt ausgerichtet (Ermittlungsbericht ***** vom *****, Anlage II.2.5).

Eine statistische Auswertung der Nutzerzahlen für die SUW GetRockMusic über die Domain ***** ergab folgendes Bild:

Der Internetdienst ***** verzeichnet für die SUW GetRockMusic im Mai 2024 372.938 Aufrufe und davon aus Deutschland ungefähr 135.265 Seitenaufrufe. In diesem Zeitraum stellten deutsche Nutzer mit 36,27 % die größte Gruppe der Nutzer dar. Für eine Ausrichtung auf

das Inland spricht weiter das herunterladbare Musikangebot. Es fanden sich im Downloadangebot der SUW die beiden erfolgreichsten Titel der deutschen Album Jahres-Charts des Zeitraums 14.06. bis 20.06.2024 und der Jahre 2020 und 2023 (Ermittlungsbericht ***** vom *****, Anhänge B und D).

Die klare Rechtsverletzung liegt in dem Bereithalten von Links, um die Titel des Tonträgers „*****“ für Nutzer des Dienstes verfügbar zu machen. Die auf GetRockMusic gelisteten Musikinhalte werden nicht auf eigenen Servern bereitgehalten, sondern können von Kunden per Hyperlink bei Sharehostern heruntergeladen werden (Ermittlungsbericht ***** vom *****, Anlage II.2.2 und Anhang A). Am ***** konnte der private Ermittler ***** das Album vollständig herunterladen und feststellen, dass es sich um das Originalalbum handelte (Ermittlungsbericht ***** vom *****, Anlage II.2.6 und Anhänge E und F).

Durch die SUW wird das nach deutschem Urheberrecht geschützte Recht verletzt, die Titel des in Rede stehenden Tonträgers von Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download öffentlich zugänglich zu machen (§ 19a UrhG). Darin liegt eine eindeutige Verletzung dieses Rechts nach § 19a UrhG (BGH, Urteil vom 12.07.2012 – I ZR 18/11 Rn. 16, 29 – Alone in the Dark; BGH, Urteil vom 15.08.2013 - I ZR 80/12 Rn. 23 ff, 46 - File-Hosting-Dienst). Dass auf der SUW ein Link bereitgehalten wird, über den der Nutzer das Musikalbum „*****“ herunterladen kann, wird durch die Anhänge A und E belegt. Danach wurde auf der SUW die Möglichkeit zum Download angeboten und dieser konnte tatsächlich durchgeführt werden.

Im Auftrag der Antragstellerin hat die Ermittlerin ***** unter der auf der SUW angegebenen E-Mail-Adresse auf unautorisierte Download-Angebote am ***** hingewiesen (Ermittlungsbericht ***** vom *****, Anlage II.5.1.2 und Anhang H). Am ***** waren die Angebote weiterhin abrufbar und die Antragstellerin ließ die Betreiber anwaltlich abmahnen (Anhang I). Am ***** waren die gemeldeten Angebote nicht mehr abrufbar. Am selben Tag meldete die Ermittlerin ***** weitere 155 unautorisierte Download-Angebote. Am ***** war die SUW zunächst nicht erreichbar, was sich allerdings am folgenden Tag wieder änderte (Ermittlungsbericht ***** vom *****, Anlage II.5.1.2). Am ***** meldete ***** insgesamt 1.241 unautorisierte Download-Angebote, darunter auch das hier in Rede stehende Musikalbum „*****“. Daran änderte sich in den folgenden Tagen nach zwei Erinnerungen nichts. Die anwaltlichen Vertreter der Antragstellerin haben die Betreiber der SUW daraufhin unter der angegebenen E-Mail-Adresse ***** erfolglos abgemahnt (Ermittlungsbericht ***** vom *****, Anlage II.5.1.2 und Anhang M).

3. Domains

Für die SUW wird die Domain „*****“ benutzt, die nach wie vor verfügbar ist (Ermittlungsbericht ***** vom *****, Anlage II.5.2.3 und Anhang A und Anhang E).

4. Subsidiarität

Die Antragstellerin muss zunächst vorrangig ihre Rechte gegenüber denjenigen Beteiligten verfolgen, die – wie die Betreiber beanstandeter Websites – entweder die Rechtsverletzung selbst begangen oder zu der Rechtsverletzung – wie der Host-Provider der beanstandeten Websites – durch die Erbringung von Dienstleistungen beigetragen haben. Ein Antrag auf Sperrung einer SUW ist daher nur zulässig, wenn der Inanspruchnahme des Betreibers der Website jede Erfolgsaussicht fehlt und deshalb andernfalls eine Rechtsschutzlücke entstünde. Der Antragsteller muss zumutbare Maßnahmen zur Aufdeckung der Identität des Betreibers der Website unternommen haben. Hier kommen insbesondere die Einschaltung der staatlichen Ermittlungsbehörden im Wege der Strafanzeige und auch die Vornahme privater Ermittlungen etwa durch einen Detektiv oder andere Unternehmen, die Ermittlungen im Zusammenhang mit rechtswidrigen Angeboten im Internet durchführen, in Betracht (vgl. BGH, Urt. v. 26.11.2015 – I ZR 174/14, GRUR 2016, 268 Rn. 83, 87 – Störerhaftung des Access-Providers; Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 27 – 31, 39 – DNS-Sperre).

Diese Voraussetzung ist im vorliegenden Fall erfüllt.

Die Identität des Betreibers der SUW ließ sich aufgrund der auf der SUW bereitgehaltenen Informationen nicht feststellen. Sie enthält kein Impressum und keine anderen weiterführenden Informationen oder Hinweise, die eine Identifizierung ermöglichen (Ermittlungsbericht ***** vom *****, Anlage II.5.1.1 und Anhang F Nr. 1).

Um die Identität des Betreibers der SUW festzustellen, hat die Antragstellerin einen privaten Ermittler beauftragt, der Dienstleister der SUW ermittelt hat. Diese sind von den Rechtsanwälten der Antragstellerin auf Auskunft in Anspruch genommen worden. Ermittelt wurden Daten zum Host-Provider, zur Zertifizierungsstelle und zum Registrar.

Der Registrar ***** wurde erfolglos vom privaten Ermittler zur Auskunftserteilung aufgefordert (Ermittlungsbericht ***** vom *****, Anlage II.5.1.2 Nr. 3 Anhang F Nr. 3 und Anhänge N sowie O). Die vom Anwalt der Antragstellerin angeschriebene Zertifizierungsstelle verweigerte eine Auskunft (Ermittlungsbericht ***** vom *****, Anlage II.5.1.2 Nr. 4).

Die vorstehend beschriebenen Auskunftersuchen gegenüber dem Registrar und dem Zertifikatanbieter führten nicht zur Identifizierung des Betreibers der SUW oder zu weiteren Ermittlungsansätzen.

Die Notifizierung und die Abmahnung des Host-Providers ***** mit Sitz in ***** einschließlich eines Auskunftsverlangens brachten keine Erkenntnisse über den Betreiber der SUW und führten nicht zu einer Beendigung der Rechtsverletzungen (Ermittlungsbericht ***** vom *****, Anlage II.5.2.2 Anhänge R und S und Ermittlungsbericht ***** vom *****, Anlage II.5.2.3 sowie Anhänge T, U, V und W). Einer weiteren Inanspruchnahme des Host-Providers fehlt jegliche Erfolgsaussicht.

Die Subsidiaritätsanforderungen, die auch eine gerichtliche Durchsetzung von Auskunftsansprüchen gegen Host-Provider mit Sitz im EU-Ausland erfordern können (BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 41 – DNS-Sperre; OLG München vom 27.05.2021 – 29 U 6933/19), sind im Streitfall nicht anwendbar, weil ***** in ***** gelistet ist und seinen Sitz außerhalb der EU hat. Eine Rechtsverfolgung im Inland gegen den in ***** ansässigen Dienstleister ist nicht erfolgversprechend. Die Durchführung eines gerichtlichen Verfahrens im Inland gegen den Host-Provider und eine Vollstreckung eines Auskunftstitels in der Ukraine sind nach der Lebenserfahrung derzeit wegen der damit verbundenen zeitlichen Verzögerung und den Schwierigkeiten einer Zustellung und Zwangsvollstreckung nicht zumutbar und nicht erfolgversprechend (vgl. BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 41 und 55 – DNS-Sperre). Anhaltspunkte, dass im vorliegenden Fall etwas anderes gilt, liegen dem Prüfungsausschuss nicht vor und sind auch sonst nicht ersichtlich. Nach der Rechtsprechung dürfen unter Berücksichtigung des für eine Rechtsverfolgung gegen Host-Provider mit Sitz außerhalb der EU geltenden großzügigen Maßstabs dem Antragsteller keine überzogenen Anforderungen an die Darlegungslast auferlegt werden (BGH, Urt. v. 13.10.2022 – I ZR 111/21, GRUR 2022, 1812 Rn. 41–DNS-Sperre; OLG München, Urt. v. 18.04.2024 – 29 U 3592/19, GRUR-RS 2024, 11885 Rn. 54).

Für die Antragstellerin besteht unter all diesen Umständen keine andere Möglichkeit, der Verletzung ihres Rechts entgegenzuwirken, als die Verhängung einer Sperrmaßnahme.

5. Zumutbarkeit und Verhältnismäßigkeit

Die DNS-Sperre ist zumutbar und verhältnismäßig.

Legale Inhalte, die auf einer SUW auch öffentlich wiedergegeben werden, stehen einer Einordnung als SUW nicht entgegen, wenn es sich in Bezug auf das Gesamtverhältnis von rechtmäßigen zu rechtswidrigen Inhalten um eine nicht ins Gewicht fallende

Größenordnung von legalen Inhalten handelt (vgl. BGH, Urt. v. 26. 11.2015 – I ZR 174/14, GRUR 2016, 268 Rn. 55 – Störerhaftung des Access-Providers) und den Internetnutzern durch eine Sperre der Webseite nicht unnötig die Möglichkeit vorenthalten wird, in rechtmäßiger Weise Zugang zu den verfügbaren Informationen zu erlangen (vgl. EuGH, Urt. v. 27. März 2014 – C-314/12, GRUR 2014, 468 Rn. 63 – UPC Telekabel/Constantin Film ua [kino.to]).

Die Verhältnismäßigkeit ist vorliegend gegeben.

Auf der SUW konnten im Rahmen einer repräsentativen Zufallsstichprobe von 100 Eintragungen aus der Grundgesamtheit aller Inhalte von 41.630 Einträgen 97 Eintragungen der repräsentativen Stichprobe als klare Urheberrechtsverletzungen ermittelt werden (Anhang G). Mit einer statistischen Wahrscheinlichkeit von 95,5 % liegt der Anteil urheberrechtswidriger Inhalte an der Grundgesamtheit zwischen 93,57 % und 100 % (Anhang G).
