Der Prüfungsausschuss

Empfehlung zur Umsetzung einer DNS-Sperre

Auf Antrag von

*****

Antragstellerin

*****

hat der Prüfungsausschuss durch

*****

als Vorsitzenden

*****

und

*****

als Beisitzer

aufgrund der Beratung vom 20. Januar 2025 einstimmig beschlossen:

Es wird empfohlen, für die Website

NXBREW

verfügbar unter

*****

eine DNS-Sperre umzusetzen.

Begründung:

A. 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.

B. 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 der 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 „game – Verband der Deutschen Games-Branche e. V.“, der Partei des Verhaltenskodexes ist und der dem Antrag zugestimmt hat (Anlage IV).

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

C. Begründetheit des Antrags

Der Antrag auf Empfehlung der Sperrung der Website NXBREW 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 NXBREW eine DNS-Sperre gemäß dem Verhaltenskodex 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 abzuhelfen, 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 Richtline (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 Richtline (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 Richtline (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 Urheberrechten im Hinblick auf das Öffentlich-Zugänglichmachen von Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download (§ 19a UrhG) an dem am 28. April 2017 veröffentlichten urheberechtlich geschützten Videospiel

*****

geschaffen von *****. Die vorgenannten Personen sind ***** Staatsangehörige und Angestellte der Antragstellerin aufgrund von Anstellungsverträgen nach ***** Recht. Diese Angestellten haben das Werk in Erfüllung arbeitsvertraglicher Pflichten und Aufgaben geschaffen. Nach § 15 des ***** Urheberrechtsgesetzes entstehen alle Urheberrechte an Werken, die ein Angestellter in Erfüllung seiner arbeitsvertraglichen Pflichten und Aufgaben schafft, automatisch bei seinem Arbeitgeber (hierzu eidesstattliche Versicherung des Rechtsanwalts Sebastian Scholl vom 10. Dezember 2024, Anl. II.1.a).

Der Antrag bezieht sich auf eine Verletzung des Urheberrechts der Antragstellerin an dem Videospiel *****. Dabei handelt es sich um ein nach § 2 Abs. 1 Nr. 1, 2 und 6, Abs. 2 UrhG geschütztes Werk (vgl. BGH, Urt. v. 6.10.2016 – I ZR 25/15, GRUR 2017, 266 Rn. 34 - World of Warcraft I; OLG Köln, GRUR 1992, 312, 313; Bullinger/Czychowski GRUR 2011, 19, 23 f).

Die Rechtsinhaberschaft der Antragstellerin ist belegt durch die übliche Angabe ihres Namens als Urheberin des erschienenen Werks auf den Vervielfältigungsstücken nach § 10 Abs. 1 UrhG (©-Vermerk auf den Vervielfältigungsstücken, Anl. II.1.b; hierzu LG Hamburg, Urteil

vom 20.07.2012 – 308 O 76/11, BeckRS 2012, 212015 Rn. 42) sowie durch eidesstattliche Versicherung (Anl. II.1.a).

2. Strukturell urheberrechtsverletzende Website (SUW)

Die Website ist in englischer Sprache gehalten (Anl. II.2.4). Sie ist gleichwohl auf den deutschsprachigen Markt ausgerichtet (Anl. II.2.5). Die Seite bietet eine Suchfunktion für bestimmte Seiteninhalte an. Bei Eingabe des Begriffs „German“ in das Suchfeld wurden Suchergebnisse angezeigt, die eine deutsche Sprachfassung oder die den Begriff „german“ im Namen aufwiesen. Für das Videospiel „*****“ wurde ebenfalls eine deutschsprachige Fassung bereitgehalten (Anl. II.2.5).

Eine statistische Auswertung der Nutzerzahlen für die SUW NXBREW ergab folgendes Bild (Anl. II.2.5):

Die SUW NXBREW belegte auf der Grundlage der vom Internetdienst SimilarWeb ermittelten Nutzerzahlen im Zeitraum von Mai bis August 2024 weltweit Rang 24.313 der am häufigsten abgerufenen Websites und in diesem Zeitraum erfolgten 5,41 % der Aufrufe aus Deutschland. Deutsche Nutzer stellten in diesem Zeitraum die viertgrößte Gruppe der Nutzer der SUW dar. In der Zeit von Mai bis August 2024 erfolgten 112.873 Besuche der SUW NXBREW aus Deutschland.

Die klare Rechtsverletzung besteht im Bereithalten von Links, um das Videospiel „*****“ für Nutzer über File-Hosting-Dienste verfügbar zu machen (Anl. II.2.6). Darin liegt eine eindeutige Verletzung des Rechts des Öffentlich-Zugänglichmachens nach § 19a UrhG (BGH, Urt. v. 12.07.2012 – I ZR 18/11, GRUR 2013, 370 Rn. 16, 29 – Alone in the Dark; BGH,

Urt. v. 15.08.2013 – I ZR 80/12, GRUR 2013, 1030 Rn. 23 ff., 46 – File-Hosting-Dienst). Durch die SUW wird das nach deutschem Urheberrechtsgesetz geschützte Recht verletzt, das in Rede stehende Videospiel von Orten und zu Zeiten nach Wahl des Internetnutzers zum permanenten Download öffentlich zugänglich zu machen.

Ein auf der SUW zu dem Videospiel „*****“ bereitgehaltener Link führte zu dem Filehoster *****, bei dem auf der Unterseite „*****“ Dateien zum Hauptspiel heruntergeladen und nach erfolgreichem Download ohne weitere Schritte entpackt und genutzt werden konnten (Anl. II.2.6).

Gegen die SUW sind in Spanien und Italien bereits gerichtliche bzw. behördliche Sperrentscheidungen verhängt worden (Entscheidung 231/2020, Juzgado de lo Mercantil n° 06 de Barcelona vom 6. Oktober 2020 und Entscheidung 29/20/CSP, Autorità per le garanzie nelle comunicazioni (AGCOM) vom 13. Februar 2020, Anl. II.2.7).

3. Domains

Für die SUW wurde zunächst die Domain „*****“ genutzt, die am 16.09.2024 verfügbar war (Anl. II.2.2, II.2.3, II.4). Derzeit verwendet die SUW die Domain „*****“, die nach wie vor verfügbar ist (Anl. II.2.3, II.4).

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. Die Antragstellerin 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 (Anl. II.5.1.1). Um die Identität des Betreibers der SUW festzustellen, hat die Antragstellerin einen privaten Ermittler beauftragt.

Zur Identifizierung der Betreiber wurden sämtliche Dienstleister der SUW ermittelt, die durch die Rechtsanwaltskanzlei ***** auf Auskunft in Anspruch genommen wurden (Anl. II.5.1.2.b). Ermittelt wurden Daten zu Host-Providern (Anl. II.5.2.1 und II.5.2.2), TLS-Zertifikat-Providern, Registraren, Registrierungsstellen (Registry) und Whois-Protection-Diensten der SUW.

Die Maßnahmen des privaten Ermittlers ***** richteten sich zunächst auf die Domain „NXBREW.COM“, die die SUW zuvor verwendet hat (Anlage II.5.1.2a). Als TLS-Zertifikat-Provider wurde „*****“, als Host-

Provider „*****.“, als Registrar „*****“, später „*****.“, als Registrant das Unternehmen „*****“, ein Verschleierungsdienst, und als Registrierungsstelle „*****“ ermittelt (Anl. II.5.1.2a).

Weiter haben der private Ermittler und die Rechtsanwaltskanzlei ***** Maßnahmen im Hinblick auf die neue Domain „*****“ ergriffen, um den oder die Betreiber der SUW zu ermitteln. Die Ermittlungsmaßnahmen haben ergeben, dass die SUW „NXBREW“ für ihre Domain „*****“ mit Ausnahme des Registrars und des Verschleierungsdienstes dieselben Intermediäre wie bei der früheren Domain „*****“ nutzt (Anlage II.5.1.2a). Als Registrar verwendet die Domain „*****“ das Unternehmen „*****.“ Als Betreiber (Registrant) wird der Verschleierungsdienst „*****“ bezeichnet (Anlage II.5.1.2a und II.5.1.2.b).

Da die Betreiber der SUW „NXBREW“ anhand der ermittelten Daten nicht identifiziert werden konnten, nahm die Kanzlei ***** die identifizierten Dienstleister der SUW auf Auskunft in Anspruch, um die Identität der Betreiber zu klären. Die Auskunftsverlangen führten nicht zur Identifizierung der Betreiber der SUW. Infolge der Notifizierung der Registrare wurde die ursprüngliche Domain „*****“ dekonnektiert und vom Registrar einbehalten. Die Betreiber der SUW wechselten daraufhin die Domain zu „*****“ und führen ihre Dienste nunmehr unter dieser Domain fort. Auch die Auskunftsgesuche zur neuen Domain und ihren Dienstleistern führten nicht zur Identifizierung der Betreiber (Anl. II.5.1.2.b).

Auf der SUW ist kein Impressum angegeben. Nach den durchgeführten Ermittlungen gehören möglicherweise die E-Mail-Adressen "*****", „*****“, „*****“, „*****“, „*****“ zum Betreiber der Seite. Es ist unklar, ob dies tatsächlich der Fall ist. Da die Kontaktierung dieser Adressen jedoch die einzige Möglichkeit darstellt, eventuell mit den Betreibern der Website in Kontakt zu treten, hat die Kanzlei ***** die

Betreiber auf diesem Wege erfolglos anwaltlich auf Unterlassung und Auskunft in Anspruch genommen (Anl. II.5.1.3.).

***** ist ein US-amerikanisches Unternehmen, das „*****“ als DDOS-Schutzdienst einsetzte. Cloudflare Inc. teilte am 16.09.2024 auf Anfrage des privaten Ermittlers mit, dass der in London ansässige Dienst „*****“ Host-Provider der Domain ist (Anl. II.5.2.2 und II.5.2.3). Die anwaltlichen Schreiben der Kanzlei ***** an *****. blieben unbeantwortet. Sie führten weder zu einer Beendigung der Rechtsverletzungen durch die SUW noch zur Identifizierung der Betreiber. Die neue Domain „*****“ wird ebenfalls von „*****“ gehostet. An der grundsätzlichen Bewertung zu diesem Provider hat sich durch den Domainwechsel nichts geändert (Anl. II.5.2.3).

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 „*****“ den Sitz außerhalb der EU hat. Eine Rechtsverfolgung im Inland gegen den in Großbritannien ansässigen Host-Provider ist wegen der mit einem solchen Verfahren verbundenen zeitlichen Verzögerung und den Schwierigkeiten einer Zustellung und Zwangsvollstreckung in Großbritannien 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).

Eine Inanspruchnahme des in Großbritannien ansässigen Dienstes „*****“ im Wege eines Verfügungsverfahrens bietet keine hinreichende Aussicht auf Erfolg. Die Rechtsverfolgung gegen den Dienst „*****“ in einem Verfügungsverfahren vor einem inländischen Gericht in der jüngerer Vergangenheit im Zusammenhang mit der Tätigkeit als

Host-Provider für eine andere Domain, über die Rechte des geistigen Eigentums verletzende Inhalte verbreitet wurden, belegt die Erfolglosigkeit eines gerichtlichen Auskunftsersuchens im Inland und dessen Durchsetzung in Großbritannien, das nicht mehr der EU angehört (Anl. II.5.2.3). „*****“ hat auf die in Großbritannien vollzogene einstweilige Verfügung des deutschen Gerichts in jenem anderen Verfahren nicht reagiert. Es ist nicht davon auszugehen, dass im Fall des Drittstaats Großbritannien gleichwertige Vollstreckungsmöglichkeiten wie in den Mitgliedstaaten der EU bestehen. 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 der Antragstellerin 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). Eine Zwangsvollstreckung eines gerichtlichen Auskunftsersuchens im vorliegenden Fall ist wegen der unklaren Rechtslage im Hinblick auf deren Durchführung in Großbritannien nach dem Austritt aus der EU und der damit verbundenen Verzögerung unzumutbar und käme einer Rechtsschutzverweigerung gleich. Einer weiteren Inanspruchnahme des Host-Providers fehlt danach jegliche Erfolgsaussicht (Anl. II.5.2.3). Zudem ist die Inanspruchnahme von Host-Providern zur Beendigung der Rechtsverletzung regelmäßig ungeeignet. Betreiber der SUW können durch einfachen Wechsel zu anderen Host-Providern die SUW weiter betreiben.

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 gegeben. Der private Ermittler hat am 27.08.2024 die SUW ausgelesen. Nach Entfernung von Duplikaten und reinen Übersichtsseiten verblieb eine Grundgesamtheit von 11.555 Einträgen. Aus dieser Grundgesamtheit hat der private Ermittler eine Zufallsstichprobe von 100 Einträgen erstellt. 96 Eintragungen der Zufallsstichprobe enthielten urheberrechtswidrige Inhalte und einen funktionierenden Downloadlink (Anl. II.3).

Mit einer statistischen Wahrscheinlichkeit von 95,5 % liegt der Anteil urheberrechtswidriger Inhalte an der Grundgesamtheit auf der Grundlage des Stichprobenergebnisses von 96 urheberrechtswidrigen Inhalten nach der Fehlertoleranztabelle

zwischen 90,4 % und 100 % und nach der approximativen Berechnungsmethode zwischen 90,0 % und 98,5 % (Anl. II.3).

Die statistische Ermittlung ist vom Geschäftsführer des privaten Ermittlers nach den Empfehlungen eines Instituts für Rechtsdemoskopie durchgeführt worden.

***** ***** *****