Position des Verbands unabhängiger Musikunternehmer*innen (VUT) zum aktuellen Diskussionsstand des europäischen Digital Services Act (DSA)

Stand: 3. März 2022

Der am 15.12.2020 vorgestellte Entwurf des Digital Service Act (DSA) ist eines der zentralen Projekte der EU-Kommission.[1] Diese überschreibt ihr Gesetzvorhaben mit „*Gesetz über digitale Dienste: mehr Sicherheit und Verantwortung im Online-Umfeld*" und weiter heißt es: „*Erstmals eröffnet ein einheitliches Regelwerk zu Pflichten und Verantwortlichkeiten von Vermittlern binnenmarktweit neue Möglichkeiten, digitale Dienste länderübergreifend anzubieten*".[2] Der DSA enthält wesentliche materielle Regelungen für Anbieter von digitalen Diensten und wurde daher auch als ein Europäisches „Grundgesetz des Internet" interpretiert.

Nachdem im November 2021 der Europäische Rat und kurze Zeit später im Januar 2022 das Europäische Parlament ihre Standpunkte vorgelegt hatten, finden seit Februar 2022 die Trilog-Verhandlungen statt. Die Verhandlungen sollen auf Drängen Frankreichs spätestens im März 2022 abgeschlossen sein.

Der VUT ist der Meinung: Der von der französischen Ratspräsidentschaft vorgegebene Zeitplan bis zum Abschluss des Trilogs reicht nicht aus, um diese weichenstellenden Regelungen für die Zukunft des Internets ausreichend zu erörtern.

In der Vergangenheit dauerte der Prozess auf vergleichbaren Gebieten (AVMD-Richtlinienänderung, DSGVO, TCO-Verordnung, DSM-Richtlinie) jeweils 1-2 Jahre. Zudem ist der DSA eine möglicherweise vollharmonisierte (Vorschlag des Rates), horizontale und nicht sektorenspezifische Verordnung mit detaillierten Regelungen. Außerdem liegen teilweise stark abweichende Vorschläge von Rat, Kommission und Parlament vor. Das Thema hat in der medialen Debatte bisher kaum stattgefunden. Obendrein liegen Regelungsvorschläge auf dem Tisch, die das Ziel „mehr Sicherheit und Verantwortung im Online-Umfeld" nicht nur verfehlen, sondern den bisherigen Schutz des Status Quo zum Teil sogar verschlechtern. Im Folgenden listen wir die aus Sicht des VUT dringendsten Veränderungen an den Entwürfen zum DSA auf.

[1] Weitere Informationen auch hier: https://emr-sb.de/themen/dma-dsa/
[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de

1 Illegale Inhalte

Die Kommission will mehr Sicherheit und Verantwortung im Internet. Stattdessen werden durch mehrere Regelungen illegale Inhalte leichter auffindbar und ihre Entfernung wird erschwert.

1.1 Kein neues Haftungsprivileg für Suchmaschinen – Artikel 4

Der Änderungsvorschlag des Europäischen Rats zu Artikel 4 soll Suchmaschinen – allen voran Google – und möglicherweise YouTube soweit es als Suchmaschine genutzt wird, generell von der Haftung freistellen. Das Europäische Parlament zielt in Erwägungsgrund 27a in die gleiche Richtung, indem es darauf hinweist, auch Suchmaschinen könnten unter bestimmten Umständen als sog. „Caching Services" (Zwischenspeicherdienste) qualifiziert werden – also Dienste, die Informationen nur technisch durchleiten. Doch gerade Suchmaschinen verlinken massenhaft auf illegale Inhalte. Sie nehmen keineswegs eine „neutrale Rolle" ein, sondern sie monetarisieren ihre Suchergebnisse und haben so einen finanziellen Anreiz, Suchende entsprechend weiterzuleiten. Sollten Suchmaschinen den Caching-Services gleichgestellt werden, wären sie in der Konsequenz **aus jeglicher Haftung für die Suchergebnisse entlassen sind – auch wenn diese auf illegale Inhalte verweisen**. Diese Regelung würde einen neuen Anreiz für Suchmaschinen schaffen, die von ihnen kuratierten und im Hinblick auf die Monetarisierung optimierten Ergebnisse noch konsequenter ausschließlich nach dem Kriterium der Maximierung ihrer Werbeeinnahmen zusammen zu stellen.

Nach geltender Rechtslage ist die Haftung von Suchmaschinen in der Europäischen Union unklar. In den USA hingegen sind Suchmaschinen gesetzlich verpflichtet auf Hinweise zu reagieren und Suchergebnisse, die auf rechtswidrige Inhalte verweisen aus ihrem Index zu entfernen (sog. „Delisting"). Vieles spricht dafür, dass nach geltender Rechtslage Suchmaschinen jedenfalls nicht wie Hosting- oder Caching-Provider in der Europäischen Union von der Haftung generell ausgenommen sind. In der Praxis hat sich ein mit den USA vergleichbares Notice & Action-Verfahren herausgebildet: Bei entsprechendem Hinweis auf illegale Inhalte reagiert der Suchmaschinenbetreiber derzeit mit „Delisting", sprich die Quelle wird auf entsprechende Suchanfragen nicht mehr angezeigt. Zu diesem Zweck haben sich spezielle Tools für das Verfahren etabliert, z. B. die Google Webmaster Tools bzw. die Google Search Console. Allein in Deutschland werden infolgedessen jährlich nicht nur aus **urheberrechtlichen Gründen** hunderttausende Webseiten aus dem Index gestrichen: Im Hinblick auf den **Jugendschutz ist „Delisting" eine unverzichtbare Unterstützung**. So werden die bekanntesten pornographischen Webseiten von den Suchmaschinen nicht gelistet und den „googelnden" Jugendlichen nicht angezeigt. In die gleiche Richtung zielt Artikel 21 Abs. 2 TCO-Verordnung: Öffentliche Aufforderungen zur Begehung einer terroristischen Straftat sind zu löschen oder, wenn das nicht möglich ist, zu sperren. Suchmaschinen reagieren auch hier mit „Delisting".

Besonders die aktuelle Lage zeigt, dass Suchmaschinen sehr wohl in der Lage sind, ihre Ergebnisse zu kuratieren, in dem sie aktiv russische Propaganda depriorisieren und entsprechende Werbung unterbinden.[3] Dieses wichtige politische Zeichen gegen den russischen Krieg zeigt auch, dass es sich nicht um rein technische Dienstleiter handelt.

Das System ist nicht perfekt und für die Verbreitung illegaler Inhalte finden Dritte in der Praxis viele Wege zum Ziel. Aber statt wie beabsichtigt die Verantwortlichkeit im Internet zu erhöhen, Sorgfaltspflichten auszubauen zumindest aber weiter zu konkretisieren, wird insbesondere vom Europäischen Rat **im krassen Gegensatz zum gesetzgeberischen Ziel ein neues Privileg für Suchmaschinen vorgeschlagen**, welches sie gänzlich aus der Verantwortung entlassen soll.

► Wir fordern, den Begriff „Suchmaschinen" aus Artikel 4 und Erwägungsgrund 27a zu streichen.

[3] https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

1.2 Entfernung Illegaler Inhalte nicht erschweren – Artikel 8.2a(ii), Artikel 14.2b, Artikel 14.3a

1.2.1 Wirksame Notice & Action-Prozesse sind Voraussetzung, um illegalen Inhalten vorzubeugen und diese schnell zu entfernen. Das Europäische Parlament will dagegen auf Kriterien wie „tatsächliche Kenntnis" und „unverzügliches Handeln" verzichten, wie sie zum Beispiel im Bereich des personenbezogenen Datenschutzes selbstverständlich sind (Artikel 5 DS-GVO). Entsprechend sollen in Zukunft während der Dauer der Prüfung ihrer Rechtmäßigkeit Inhalte grundsätzlich zugänglich bleiben. Dies gilt selbst, wenn es sich um offensichtlich rechtswidrige Inhalte wie Anleitungen zum Bombenbau, Pornographie, rassistische Hetze, Live-Fußballspiele auf Social Media-Kanälen oder wiederholt urheberrechtsverletzende Angebote handelt. Diese Regelung ist weder sachgerecht noch verhältnismäßig. Offen bleiben Konflikte sowohl mit bestehenden Verordnungen und Richtlinien im Falle einer Vollharmonisierung als auch wenn wie vom Europäischen Parlament vorgeschlagen (Erwägungsgrund 9) die Kommission Leitlinien zur Auslegung der Wechselbeziehungen und zur Vermeidung von Konflikten bei der Auslegung erarbeiten soll.

► Wir fordern den vom Europäischen Parlament vorgeschlagenen Artikel 14.3a(neu) abzulehnen, um die Verfahren nicht zu verzögern.

1.2.2 Das Parlament schlägt vor, dass bei der Meldung eines rechtsverletzenden Inhalts als Obliegenheit eine eindeutige Angabe des genauen elektronischen Speicherorts – etwa eine präzise URL-Adresse – angegeben werden muss und falls dies angemessen ist oder wenn der genaue elektronische Speicherort nicht präzise ermittelbar ist, eine oder mehrere präzise URL-Adresse(n) (Uniform Resource Locator) und nötigenfalls weitere Angaben zur Ermittlung der betreffenden illegalen Inhalte ausreichen. Der Europäische Rat fordert allgemein Informationen, die dem Anbieter das Auffinden des rechtswidrigen Inhalts ermöglicht und nennt beispielhaft – aber nicht zwingend (!) – präzise URL-Adressen. Wäre die Angabe einer URL-Adresse zwingende Handlungsvoraussetzung, wären über Apps zugänglich gemachte rechtsverletzende Inhalte generell aufgrund der konkreten Art einer App nicht identifizierbar, die Regelung würde dort nicht greifen.

► Wir fordern die Klarstellung, dass präzise URL-Adressen nicht unbedingte Voraussetzung für das Handeln eines Anbieters sind.

1.3 Wiederholungstäter zur Verantwortung ziehen – Artikel 20.1

Ein wichtiges Instrument, um die Online-Sicherheit zu gewährleisten und illegale Inhalte zu bekämpfen, sind verbindliche und verpflichtende Maßnahmen gegen Wiederholungstäter. Dies wird von der Kommission und vom Rat bestätigt. Das Parlament untergräbt diese Regelung jedoch, indem es hinzufügen möchte, Plattformen seien lediglich „berechtigt", Wiederholungstäter für eine gewisse Zeit von ihren Diensten auszusetzen.

► Wir unterstützen den Ansatz von Rat und Kommission, der Vorschlag des Parlaments zu Artikel 20.1 sollte unberücksichtigt bleiben.

1.4 Keine Verschlechterung der Rechtsdurchsetzung – Artikel 7

Das Europäische Parlament möchte das generelle Verbot einer allgemeinen Verpflichtung zur Überwachung umfangreich konkretisieren. Weder de jure noch de facto soll das Verhalten natürlicher Personen mit automatischen Hilfsmitteln überwacht werden, anonyme Nutzung und Ende-zu-Ende-Verschlüsselung werden adressiert. Die bisher allgemeine Schranke (Artikel 15 E-Commerce-RL), ihrerzeit zur Untermauerung der Haftungsprivilegien eingeführt, wurde inzwischen mit guten Argumenten relativiert (siehe AVMD-RL, DSM-RL, TCO-VO, TTDSG und BGB-Reform sowie das Netz-DG mit den dort verankerten Löschpflichten). Der Bundesgerichtshof hat

eine Klarnamenpflicht im Innenverhältnis bestätigt.[4] Die vom Europäischen Parlament vorgeschlagene Konkretisierung erweitert das allgemeine Verbot gegen den Trend einer sektorenspezifischen präziseren Ausbalancierung der verfassungsrechtlich geschützten Grundrechtspositionen.

►Der von Rat und Kommission vorgelegte Text sollte beibehalten werden.

1.5 Unmittelbare Verantwortlichkeit der Vermittlungsdienste erhalten

Der schnellste, direkteste und effektivste Weg Rechtsverletzungen abzustellen und weiteren Schaden zu vermeiden, ist die Durchsetzung von (verschuldensunabhängigen) Unterlassungsansprüchen gegen den Vermittlungsdienst. Dieser Anspruch ist sinnvoll, bewährt, in Artikel 14 Abs. 3 der E-Commerce-RL bestätigt und nun in Artikel 5.4 bekräftigt. In Erwägungsgrund 26 wird vorgeschlagen, „wenn möglich sollten Dritte, die von im Internet übertragenen oder gespeicherten illegalen Inhalten betroffen sind, versuchen, Konflikte im Zusammenhang mit solchen Inhalten beizulegen, ohne die betreffenden Anbieter von Vermittlungsdiensten zu beteiligen“. Eine Lesart könnte sein, dass Ansprüche grundsätzlich zunächst gegen die Täter*innen einer Rechtsverletzung bzw. die Endnutzer*innen zu richten sind. Ein entsprechendes Vorgehen ist weder sinnvoll noch angemessen, denn Endnutzer*innen haben oft nicht die Mittel, um eine Rechtsverletzung unmittelbar zu beenden und solange sie anonym agieren können, sind sie oft auch nicht motiviert, entsprechende Maßnahmen zu ergreifen. Artikel 5 Abs. 4 sollte nicht durch Erwägungsgrund 26 relativiert werden.

► Die Änderungsvorschläge des Parlamentes zu den Artikeln 14.6 und 8.2cb und den Erwägungsgründen 40a und 40b sollten abgelehnt und der Text der Kommission beibehalten werden.

1.6 Expertise der Rechteinhaber als „Trusted Flagger“ nutzen – Artikel 19.2b

Der VUT vertritt die Interessen von ca. 1.200 Musikunternehmer*innen. Unsere Mitglieder kennen ihre Kataloge bzw. Rechte sowie die praktizierten Verfahren und Prozesse besser als Verbände oder die Politik. Unsere Mitglieder haben mehrere tausend Mitarbeiter*innen und die meisten von ihnen sind mit dem Fachwissen eines „Trusted Flagger“ gemäß Artikel 19.2a des Entwurfs der Kommission ausgestattet. Das heißt: Unsere Mitglieder sind selbst in der Lage, rechtzeitig, sorgfältig und objektiv im Sinne des Artikel 19.2c die notwendigen Informationen zu übermitteln und die Prozesse einzuhalten. Die vorgeschlagene Beschränkung des “Trusted Flagging” ausschließlich auf Organisationen, die kollektive Interessen vertreten, ist weder hilfreich noch geeignet im Sinne des Regelungszwecks: Ein Verband wie der VUT wäre ohne erhebliche zusätzliche Ressourcen nicht imstande, die Rolle eines “Trusted Flagger” nur im Ansatz zu erfüllen. Insbesondere kleine, mittelständische Unternehmer*innen, selbstvermarktende Künstler*innen und deren Verbände hätten somit keine Möglichkeit von dieser Regelung zu profitieren, wenn ihnen die Möglichkeit genommen wird, selbst zu handeln.

► Wir unterstützen die Position des Rates in Artikel 19.2b, der „Trusted Flagger“ nicht auf kollektive Interessenvertretungen einschränkt.

1.7 Kein Verbot des automatisierten Monitorings („Good-Samaritan-Clause“) Artikel 6

Seit fast 25 Jahren erleben wir die Praxis, Konkretisierung, Ausdifferenzierung und tendenzielle Verschärfung der Haftungsregelungen von Vermittlungsdiensten. Das Gesetzesvorhaben des DSA mit dem erklärten Ziel, mehr Sicherheit und Verantwortung im Online-Umfeld zu schaffen, sollte sich in diese Entwicklung einreihen und doch besteht eine bemerkenswerte Einigkeit

[4] BGH Urt. v. 27.1.2022, Az. III ZR 3/21 u 4/21

zwischen Kommission, Rat und Parlament darin, ein weiteres Haftungsprivileg in Form einer „Good-Samaritan-Clause“ („guter Samartier-Klausel“) einzuführen, wie sie im US-amerikanischen Recht gebräuchlich ist. Grundsätzlich gibt es sicher Argumente, durch die Belohnung einer Haftungsprivilegierung Akteure zu Wohlverhalten zu motivieren. Das kann aber nur gelten, wenn dieses Wohlverhalten konkret geeignet ist, das gewünschte Ziel zu fördern. Gänzlich unverständlich ist in diesem Zusammenhang daher die Ergänzung des Parlaments, das den Einsatz automatisierter Verfahren in diesem Zusammenhang ausschließen will. Ganz offensichtlich hat das Parlament nicht die Wirksamkeit der Maßnahmen im Fokus, die Ergänzung in Artikel 6.1a verfolgt vielmehr die Absicht, Overblocking („…und nicht dazu führen, dass zu viele Inhalte entfernt werden“) um jeden Preis zu verhindern. Eine Verhältnismäßigkeitsprüfung wird nicht vorgenommen. Mit Umsetzung der DSM-RL wurde von Gegner*innen insbesondere der Umsetzung von Artikel 17 eine spürbare Zunahme oder Einführung der Filterungen von Inhalten und Overblocking vorhergesagt. Offensichtlich sind diese nicht eingetreten, die Befürchtungen gingen ins Leere. Man kann inzwischen als allgemein bekannt und akzeptiert voraussetzen, dass automatisierte Verfahren zum Erkennen, Kuratieren, Empfehlen und Organisieren von Inhalten elementarer Bestandteile und geradezu Voraussetzung aller zeitgemäßen Plattformen, vor allem der besonders großen Plattformen, sind. Sie haben ihre Grenzen dort, wo eine Inhalte-Moderation durch den Menschen für den Schutz der Meinungsfreiheit unerlässlich ist. Wenn rechtsverletzende Inhalte jedoch durch automatische Hilfsmittel zuverlässig erkannt werden können, ist ihr Einsatz sinnvoll, gerechtfertigt und sollte nicht kategorisch ausgeschlossen werden.

► Artikel 6 sollte nicht um den vom Europäischen Parlament vorgeschlagenen Absatz 1a ergänzt werden.

2 “Know your Business Customer”-Regel sinnvoll ausweiten

Die Entwürfe zum DSA sehen KYBC-Regelungen („Know your business costumer“, „kenne deinen Geschäftskunden“) nur für Online-Marktplätze vor. Täglich nutzen EU-Bürger*innen gewerbliche Angebote von Online-Plattformen; Online-Marktplätze sind nur ein kleiner Ausschnitt des Angebots. Um Betrug, den Handel mit Fälschungen und illegalen Inhalten wirksam zu verhindern, ist die Ausweitung dieser Regelungen auf alle Online-Plattformen notwendig. Die Schäden allein aufgrund von Betrug mit Kryptowährungen in Deutschland belaufen sich auf hunderte Millionen Euro. Auf der einen Seite sind die Täter*innen in der Regel nicht ermittelbar, weil sie anonym agieren können.[5] Auf der anderen Seite werden die Transparenzanforderungen bei wirtschaftlichen Transaktionen laufend erhöht und sämtliche wirtschaftlich Berechtigte müssen regelmäßig bis zu den natürlichen Personen ermittelt werden (§ 3 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten - GwG).

Um mehr Transparenz, weniger Straffreiheit, eine zeitgemäße Regelung im Lichte des sonstigen Regelungsumfelds zu schaffen und somit letztlich eine bessere Durchsetzung von Rechten nicht zu erschweren, sollte der Gesetzgeber das Signal des Parlaments in EWG 39b aufgreifen und in einem neuen Artikel 13b die Regelung auf alle Vermittlungsdienste ausweiten. Viele Länder[6], darunter Italien, Spanien, Österreich, Dänemark, Portugal, Niederlande, setzen sich für die Ausweitung der Regelung ein. Entsprechende Änderungsantrage 512 und 514 scheiterten nur knapp[7] – unter anderem an einer fälschlich abgegebenen Stimme im Parlament (der Abgeordnete korrigierte dies im Nachhinein, allerdings konnte diese Änderung nicht gezählt werden).

---

[5] https://www.br.de/nachrichten/wirtschaft/betrug-mit-kryptowaehrungen-warnsystem-mit-luecken,SxQFSwO https://www.br.de/radio/bayern2/sendungen/radiofeature/die-bitcoin-falle-abzocke-mit-krypto-waehrungen-100.html

[6] https://data.consilium.europa.eu/doc/document/ST-13203-2021-ADD-1/x/pdf

[7] https://www.europarl.europa.eu/doceo/document/PV-9-2022-01-19-RCV_FR.pdf S. 96, S. 241 ff.

►Wir fordern, dass im Geist der Änderungsanträge die KYBC-Regelung auf Online-Marktplätze ausgeweitet wird.