

An das
Bundesministerium für Justiz
Museumsstraße 7
1070 Wien

Wien, am 24.08.2026

ISPA-Stellungnahme betreffend die Empfehlungen zur Bekämpfung der Online-Piraterie bei Sport- und anderen Live-Veranstaltungen

Sehr geehrter Damen und Herren,

die ISPA – Internet Service Providers Austria – begrüßt die Möglichkeit, zur Evaluierung der Empfehlung zur Bekämpfung der Online-Piraterie bei Sport- und anderen Live-Veranstaltungen Stellung zu nehmen. Als Dachverband von rund 220 österreichischen Internetdiensteanbietern vertreten wir Anbieter entlang der gesamten Wertschöpfungskette des Internets.

Die ISPA erkennt an, dass die rechtswidrige Verbreitung von Live-Inhalten, insbesondere von Sportveranstaltungen, Rechteinhaber vor erhebliche Herausforderungen stellt, äußert jedoch erhebliche Bedenken hinsichtlich der von bestimmten Rechteinhabern und einzelnen Mitgliedstaaten verfolgten Ansätze zur Anordnung und Umsetzung von Netzsperrern. Solche Maßnahmen drohen das Ziel einer ausgewogenen, wirksamen und verhältnismäßigen Bekämpfung illegaler Verbreitungen von Live-Inhalten zu untergraben.

Nicht alle Diensteanbieter sind gleichermaßen in der Lage, Rechtsverletzungen zeitnah, wirksam und verhältnismäßig zu unterbinden. **Internetzugangsanbieter sind grundsätzlich am weitesten von der eigentlichen Rechtsverletzung entfernt.** Sie stellen lediglich die Übertragungsinfrastruktur bereit, die sowohl Rechteinhaber als auch Rechtsverletzer zur Verbreitung von Inhalten nutzen. Internetzugangsanbieter können auf behördliche Anordnungen lediglich durch Sperrung ganzer Domains oder IP-Adressen reagieren – nicht jedoch durch Entfernung einzelner rechtsverletzender Inhalte.

Die Problematik von IP-Sperren hat sich in Österreich bereits sehr deutlich und eindringlich gezeigt. Im August 2022 wurden mehrere österreichische Internetzugangsanbieter von Vertretern der Musik- und Filmwirtschaft zur Sperre bestimmter IP-Adressen aufgefordert. Infolge dieser Sperren waren jedoch nicht nur die beanstandeten Inhalte, sondern auch zahlreiche rechtmäßige Websites – darunter Online-Shops, Nachrichtenangebote und Websites von NGOs – nicht mehr erreichbar,

da die betroffenen IP-Adressen von einem Content-Delivery-Network für unterschiedliche Dienste gemeinsam genutzt wurden. Neben Haftungsfragen ergaben sich daraus auch erhebliche wirtschaftliche Probleme.

Die Telekom-Control-Kommission (TKK) stellte in zahlreichen Aufsichtsverfahren gemäß Art 5 Abs 1 TSM-VO fest, dass die eingerichteten IP-Sperren gegen die Vorgaben der Netzneutralität verstoßen und daher aufzuheben sind.¹ Analog zur stets vertretenen Position der ISPA und der gesamten Branche, führte auch die Behörde dabei aus, dass zwischen IP-Adressen und Domains aus technischer Sicht keine eindeutige Zuordnung besteht: Unter einer einzigen IP-Adresse kann eine praktisch unbegrenzte Anzahl voneinander unabhängiger Websites und Dienste betrieben werden. Weder für die Regulierungsbehörde noch für die betroffenen Internetzugangsanbieter ist es möglich, verlässlich und abschließend festzustellen, welche Inhalte und Dienste von einer IP-Sperre erfasst werden – weder im Zeitpunkt der Einrichtung noch zu einem späteren Zeitpunkt.

Die TKK gelangte ferner zu dem Ergebnis und Spruchpraxis, dass IP-Sperren im Vergleich zu DNS-Sperren unverhältnismäßig sind: Beide Maßnahmen können mit vergleichbar geringem technischem Aufwand – etwa durch Nutzung eines VPN-Dienstes – umgangen werden. IP-Sperren greifen jedoch erheblich intensiver in die Grundrechte unbeteiligter Dritter ein, da sie nicht nur den Zugang zu einer konkreten Website, sondern potenziell zu sämtlichen unter der gesperrten IP-Adresse erreichbaren Diensten unterbinden.

Im Rahmen des vom Bundesverwaltungsgericht eingeleiteten Vorabentscheidungsverfahrens vor dem EuGH (verbundene Rechtssachen C-832/24 bis C-834/24) bekräftigte die TKK in ihrem Schriftsatz vom Februar 2025 diese Rechtsauffassung. In der Rechtssache C-833/24 wurden die Beschwerden der Rechteinhaber beim Bundesverwaltungsgericht zwar zurückgezogen – aber offenkundig vor dem Hintergrund, dass mit einer für die beschwerdeführenden Rechteinhaber negativen Entscheidung zu rechnen war.

Der österreichische Fall verdeutlicht, dass IP-Sperren aufgrund ihrer inhärenten technischen Unschärfe kein verhältnismäßiges Instrument zur Bekämpfung von Urheberrechtsverletzungen darstellen und zwangsläufig zu erheblichem Overblocking führen.

Zu Frage 1: Bedarf an zusätzlichen Maßnahmen

a) Regelungsbedarf nach Inhaltsarten

Die ISPA sieht derzeit keinen hinreichenden Anlass, auf EU-Ebene neue spezifische Sperrpflichten

¹ [Regulierungsbehörde untersagt im Sinne der Netzneutralität überschießende IP-Sperren | RTR](#)

für Anbieter von Internetzugangsdiensten zur Bekämpfung der Online-Piraterie von Live-Inhalten einzuführen. Der bestehende Rechtsrahmen ermöglicht bereits gezielte Maßnahmen gegen rechtsverletzende Angebote, insbesondere gegenüber Website-Betreibern und Hosting-Providern. Sperranordnungen gegenüber Access-Providern sollten ausschließlich als **ultima ratio** zum Einsatz kommen, wenn keine gleich wirksamen, weniger eingriffsintensiven Maßnahmen zur Verfügung stehen und eine verhältnismäßige, technisch präzise Umsetzung ohne Beeinträchtigung rechtmäßiger Inhalte und der Rechte Dritter gewährleistet ist. Entscheidend ist dabei nicht die Art der betroffenen Inhalte, sondern die grundrechtskonforme Ausgestaltung der jeweiligen Maßnahme.

Zudem sollte zunächst die weitere Konsolidierung der praktischen Umsetzung des Digital Services Act (DSA) abgewartet und dessen Wirksamkeit bei der Bekämpfung der Online-Piraterie evaluiert werden. Ein zusätzlicher unionsrechtlicher Handlungsbedarf sollte erst auf Grundlage konkret festgestellter Umsetzungsdefizite geprüft werden.

b) Geeignete Maßnahmen auf EU-Ebene

Die wirksamste Bekämpfung erfolgt **an der Quelle**. Das Internet ist global und redundant aufgebaut; Sperren durch Netzbetreiber werden daher den Zugriff auf rechtsverletzende Inhalte nicht dauerhaft verhindern können. Die einzige Möglichkeit, den Zugang zu solchen Inhalten wirksam zu unterbinden, besteht in ihrer Entfernung auf Hostingebeane durch Notice-and-Takedown-Verfahren.

Rechteinhaber sollten daher vorrangig **die tatsächlichen Rechteverletzer und Website-Betreiber sowie erst in weiterer Folge Hosting-Provider**, in Anspruch nehmen. Art. 14 DSA hat das Versenden und Empfangen entsprechender Hinweise an Hosting-Provider bereits vereinfacht.

Technische Schutzmaßnahmen wie **digitale Wasserzeichen und dynamische Steganographie** ermöglichen es Rechteinhabern, einzelne Streams individuell zu kennzeichnen. Bei Feststellung einer illegalen Weiterverbreitung kann der betreffende Nutzer identifiziert, gesperrt und schadenersatzpflichtig gemacht werden – ein wesentlich gezielteres und wirksameres Instrument als großflächige Netzsperrungen.

Forderungen nach einer Ausweitung der KYBC-Verpflichtung (Know Your Business Customer – Art. 30 DSA) auf sämtliche Intermediäre – einschließlich VPN- und DNS-Anbietern – lehnt die ISPA entschieden ab. Eine solche Ausweitung würde eine im Rahmen des DSA bereits abgeschlossene gesetzgeberische Entscheidung erneut infrage stellen und zu erheblicher Rechtsunsicherheit führen. Bevor neue Verpflichtungen eingeführt werden, müssen daher die rechtlichen und

technischen Besonderheiten der jeweils betroffenen Anbieter sorgfältig geprüft werden.

c) Grundrechtliche Schutzvorkehrungen

Die ISPA warnt nachdrücklich davor, Intermediären Entfernungs- oder Sperrpflichten innerhalb von Fristen aufzuerlegen, die eine angemessene Prüfung der beanstandeten Inhalte verhindern.

Vorschläge, Inhalte innerhalb von 30 Minuten zu sperren, würden zwangsläufig zu Overblocking führen. Intermediäre – insbesondere KMU – hätten nicht ausreichend Zeit, die Rechtswidrigkeit zuverlässig festzustellen. Um Haftung und hohe Geldbußen zu vermeiden, wären sie gezwungen, Inhalte vorsorglich zu sperren – mit dem erheblichen Risiko, auch rechtmäßige Inhalte zu erfassen.

Jede Maßnahme muss mit **Art. 10 EMRK und der EU-Grundrechtecharta** vereinbar sein. Der EGMR hat bereits klargestellt, dass IP-Sperren, die auch legale Inhalte erfassen, einer ausreichenden Rechtsgrundlage entbehren und einen ungerechtfertigten Eingriff in die Informationsfreiheit darstellen (*European Court of Human Rights, Application no. 10795/14 Vladimir Kharitonov v. Russia*).

Nach der **Netzneutralitäts-Verordnung (2015/2120)** dürfen Internetzugangsanbieter nur aufgrund von Unionsrecht, nationalem Recht oder behördlichen bzw. gerichtlichen Anordnungen in den Datenverkehr eingreifen. Private Meldungen von Rechteinhabern ohne behördliche Überprüfung genügen diesen Anforderungen nicht.

Zudem ist festzuhalten: Auch wenn eine Sperre von einem Gericht oder einer zuständigen Behörde angeordnet wird und dabei sämtliche grundrechtliche Schutzvorkehrungen eingehalten werden, dürfen die mit ihrer Umsetzung verbundenen Kosten nicht einseitig auf die betroffenen Diensteanbieter überwälzt werden. Diese Mitwirkung Privater an einer staatlichen Aufgabe oder im Interesse des Staates bzw. eines Staatsunternehmens ist nach der Rechtsprechung des VfGH aufgrund des Verhältnismäßigkeitsgrundsatzes, insbesondere im Rahmen der Güterabwägung (Verhältnismäßigkeit im engeren Sinn), verfassungsrechtlich nur zulässig, wenn ein Kostenersatz vorgesehen wird (VfGH 27.2.2003, G 37/02). An dieser Rechtsprechung hat sich nichts geändert. Sie ist daher weiterhin geltendes Recht, weshalb es aus unserer Sicht zwingend geboten ist, einen entsprechenden Kostenersatz vorzusehen. Dies umfasst sowohl die erforderlichen Personal- und Infrastrukturkosten als auch die Kosten der technischen Umsetzung und des laufenden Betriebs. Eine solche Kostenregelung ist insbesondere angesichts der großen Zahl kleiner Access-Provider erforderlich, für die die Umsetzung belastender Sperranordnungen mit erheblichen organisatorischen und finanziellen Aufwendungen verbunden und daher völlig unverhältnismäßig

wäre.

Zu Frage 2: Grenzüberschreitende Zusammenarbeit

Die ISPA befürwortet **kooperative Ansätze** zwischen Rechteinhabern und Intermediären. Diese sind wirksamer als eine ausschließliche Abstützung auf gerichtliche Anordnungen. Rechteinhaber sollten unmittelbar mit Internetdiensteanbietern zusammenarbeiten, anstatt primär rechtliche Schritte gegen diese einzuleiten.

Abzulehnen sind hingegen Bestrebungen, Sperranordnungen extraterritorial auf global agierende Infrastrukturdienstleister (VPN-, DNS-Anbieter) auszuweiten, die weder im Anordnungsstaat ansässig noch dessen Jurisdiktion unterworfen sind. Eine solche Ausweitung wäre rechtlich mangels entsprechender Hoheitsgewalt und Durchsetzbarkeit ohnehin nicht möglich.

Vorschläge, wonach Intermediäre wie Internetdiensteanbieter oder Cloud-Infrastrukturanbieter – die weder Einblick in noch Kontrolle über die übertragenen Inhalte haben – diese aktiv überwachen sollen, stehen im grundlegenden Widerspruch zu den Prinzipien des DSA und kollidieren mit dem europäischen Datenschutzrecht.

Zu Frage 3: Weitere zu berücksichtigende Aspekte

Das italienische „Piracy Shield“ als Negativbeispiel

Die ISPA möchte insbesondere auf die Gefahren spezifischer Regelungen gegen Online-Piraterie von Live-Inhalten hinweisen. Das italienische „Piracy Shield“ illustriert die gravierenden Probleme überhasteter Regulierung:

Gefahr des Overblocking: Das System ermöglicht es, gemeldete Domains und IP-Adressen automatisiert an Internetzugangsanbieter zu übermitteln, die diese innerhalb von 30 Minuten sperren müssen. Da hinter einer IP-Adresse häufig viele völlig unabhängige Websites oder Dienste liegen, werden zwangsläufig auch legale Angebote mitgesperrt.

- Im **Februar 2024** führte die Sperre einer Cloudflare-IP-Adresse dazu, dass zehntausende Websites für italienische Nutzer nicht mehr erreichbar waren.
- Im **Oktober 2024** wurde Google Drive für über zwölf Stunden blockiert. AGCOM bestätigte selbst, dass die Sperrmeldung fehlerhaft war.

Die kurze Frist von 30 Minuten lässt kaum Zeit für eine Prüfung; auch dadurch kommt es zwangsläufig zu Fehlern.

Mangelnder Rechtsschutz: Betroffene Website-Betreiber haben keine realistische Möglichkeit,

eine Sperre vor deren Wirksamwerden anzufechten. Die Internetzugangsanbieter können in diesem Zeitraum praktisch nicht überprüfen, ob eine gemeldete IP-Adresse tatsächlich ausschließlich oder überwiegend für Piraterie genutzt wird. Das Haftungsrisiko wird dadurch ungebührlich auf die Internetzugangsanbieter überwältzt, während die Entscheidung faktisch auf Rechteinhaber bzw. deren Meldungen verlagert wird.

Technisch ungeeignetes Instrument: Insbesondere IP-Sperren bei Shared Hosting, Content-Delivery-Networks, DDoS-Schutzdiensten und wiederverwendeten IP-Adressen sind technisch höchst problematisch. In Österreich hat die Regulierungsbehörde nach einem Overblocking-Vorfall im August 2022 IP-Adress-Sperren aufgrund der damit verbundenen Risiken für unzulässig erklärt.

Fragliche Effektivität: Piraten können rasch auf neue Domains, IP-Adressen oder IPv6 ausweichen. Großflächige Netzsperrungen sind daher kein wirksames Instrument. Wirksamer wären gezielte Maßnahmen gegen Hosting-Anbieter bzw. die eigentlichen Betreiber.

Ausweitung des Systems: Seit 2025 wurde das Piracy Shield über Sport hinaus auf weitere live übertragene audiovisuelle Inhalte ausgeweitet. AGCOM beabsichtigt außerdem, das System auf VPN- und DNS-Anbieter auszudehnen – ohne zu berücksichtigen, dass diese ihre Dienste weltweit erbringen und vielfach nicht der italienischen Rechtsordnung unterworfen sind.

Dynamische und Live-Sperranordnungen

Dynamische Sperranordnungen bringen Internetzugangsanbieter in eine schwierige Lage: Sie müssen eigenständig beurteilen, ob zusätzliche, von Rechteinhabern gemeldete Domains tatsächlich denselben Dienst betreffen, der von der ursprünglichen Anordnung erfasst ist. Eine bloße Meldung durch Rechteinhaber stellt keine ausreichende Grundlage für Eingriffe in den Datenverkehr im Sinne der Netzneutralitäts-Verordnung dar.

Live-Sperren binnen 30 Minuten – insbesondere bei Sportereignissen an Wochenenden und außerhalb der Geschäftszeiten – erfordern eine 24/7-Verfügbarkeit von technischem und juristischem Personal. Dies ist für KMU praktisch nicht umsetzbar und verursacht unverhältnismäßige Kosten.

Erhaltung eines sicheren und offenen Internets

Die Integrität und Funktionsfähigkeit der Internetinfrastruktur sind von zentraler Bedeutung. Maßnahmen, die Anbietern auferlegt werden, können Auswirkungen auf sämtliche Nutzer haben und dabei rechtmäßige Angebote sowie grundrechtlich geschützte Interessen beeinträchtigen.

Die ISPA fordert die Europäische Kommission daher auf, einen kooperativen Ansatz zu verfolgen,

der auf einer engen Zusammenarbeit zwischen den betroffenen Wirtschaftsteilnehmern und den zuständigen staatlichen Stellen beruht. Vorrangig sollten dabei wirksame Verfahren zur Entfernung rechtswidriger Inhalte an der Quelle weiterentwickelt und genutzt werden.

Die ISPA fordert daher:

1. **Von der Empfehlung dynamischer Sperranordnungen oder sogenannter Live-Sperranordnungen abzusehen.** Diese führen zwangsläufig zu Overblocking, mangelndem Rechtsschutz und unverhältnismäßigen Belastungen für Intermediäre.
2. **Sperranordnungen gegen Internetzugangsanbieter als ultima ratio zu behandeln.** Solche Maßnahmen sollten nur erfolgen, wenn keine anderen Mittel verfügbar sind, sie angemessen umgesetzt werden können und keine Gefahr besteht, dass Rechte Dritter verletzt werden.
3. **Die vollständige Umsetzung des DSA abzuwarten,** bevor weitere regulatorische Maßnahmen in Betracht gezogen werden.
4. **Priorität auf die Bekämpfung an der Quelle zu legen** – durch Maßnahmen gegen die tatsächlichen Betreiber illegaler Angebote.
5. **Jede Maßnahme an den Grundsätzen der Verhältnismäßigkeit, der gerichtlichen bzw. behördlichen Anordnung und des angemessenen Rechtsschutzes für Betroffene auszurichten.**

Für Rückfragen stehen wir ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen



Mag. Stefan Ebenberger
Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 220 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.