EuroISPA contribution
to the Targeted initiative to support the CDSM review process

EuroISPA welcomes the opportunity to respond to the targeted initiative for a better copyright environment, aiming to collect the information necessary to support the review of the Copyright in the Digital Single Market Directive (CDSM Directive, EU 2019/790).Our members, ranging from large telecoms operators to small and medium-sized hosting providers, access providers, CDN operators, DNS resolvers, and VPN providers, sit at the heart of the digital infrastructure that underpins both the creative economy and the broader EU digital single market.

EuroISPA shares the Commission's commitment to an effective, fair, and future-proof copyright framework, and supports the protection of intellectual property rights. We recognise the real harm that online piracy causes to rightsholders and the broader creative economy. At the same time, we have a responsibility to ensure that enforcement measures are technically sound, legally proportionate, and compatible with the open and global nature of the Internet that our members help to sustain. Consistent with the Commission's Better Regulation principles, any consideration of policy options should be grounded in a clearly defined and evidence-based problem statement that broadly considers all relevant stakeholders.

This submission addresses three areas of direct relevance to our members: first, the ongoing challenges posed by network-level blocking in the context of online piracy of live events; the second, the implications of generative AI for the text and data mining framework established by Articles 3 and 4 of the CDSM Directive; the third, ensuring a common approach with the European private copying exception . While these are distinct policy questions, they share a common thread: effective copyright policy must be proportionate, evidence-based, and directed at actors who have the practical ability to act, consistent with the standards that EU law already provides through Directive 2004/48/EC (IPRED), Directive 2001/29/EC (the InfoSoc Directive), Regulation (EU) 2022/2065 (the Digital Services Act), and Directive (EU) 2019/790 (the CDSM Directive itself).

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56

ISPs and Online Piracy

The Commission's own assessment of the 2023 Recommendation on combating piracy of live events found that it had limited positive effects and did not lead to a substantial reduction of piracy. This finding is an important baseline for this consultation: it suggests that in many cases the problem lies in the enforcement of existing law, not in a gap in the legislative framework. EuroISPA urges the Commission to proceed from this baseline before introducing new enforcement obligations.

Consistent with this, EuroISPA urges the Commission to give priority to the full and consistent implementation of the Digital Services Act before introducing new enforcement obligations in this area. The DSA provides a comprehensive and carefully balanced horizontal framework for intermediary liability and notice-and-action procedures, and its impact has not yet been fully realised across all 27 Member States. The Commission has already referred several Member States to the Court of Justice for failing to effectively transpose the DSA, a reminder that the problem in many cases is one of implementation of existing law, not a gap in the legislative framework itself.

EuroISPA is deeply concerned by the approach taken in certain Member States, most notably Italy, Spain, France and Austria, as detailed in the **case studies below,** where network blocking measures have escalated beyond local access providers to target global infrastructure providers with no direct relationship to the infringing content. These approaches are neither effective nor proportionate, and risk causing significant collateral damage to lawful users and services.

EuroISPA believes that it is essential that policymakers understand the structural limitations of network-level blocking as an enforcement tool. ISPs providing access infrastructure are the furthest from the point of infringement. They can only respond to orders by blocking domain names or IP addresses; they cannot remove individual pieces of infringing content, which can only be accomplished at the hosting level through notice-and-takedown procedures. Because the Internet is designed to be global and redundant, domain or IP blocking is inherently incomplete and prone to over-blocking. This structural reality is confirmed by independent analysis: an April 2026 study by the Centre for European Policy Studies (CEPS) concludes that IP-based blocking is structurally overinclusive, that rightsholders bear none of the implementation costs and therefore have no incentive to avoid collateral damage, and recommends that IP-address blocking be avoided altogether in favour of DNS- or URL-level mechanisms where blocking is used at all.

EuroISPA would like to propose the following recommendations:

1. Exhaust existing remedies before introducing new obligations

EuroISPA believes that before introducing additional legislation or expanding technical enforcement mandates, policymakers should carefully evaluate whether more effective implementation of existing copyright law, in particular the injunctive remedies already available under Article 8(3) of the InfoSoc Directive and Articles 9 and 11 of IPRED, combined with enhanced coordination with stakeholders, could better address many of the identified concerns.

In this context, the experience of the Digital Services Act (DSA), in force since 2022, is particularly relevant. While the DSA strengthens the framework for addressing illegal content online, including copyrighted material and illegal live streams, its application should first be assessed in practice before considering new sector-specific enforcement obligations.

This targeted legislative initiative represents an opportunity to clarify and improve the calibration of these existing remedies, rather than to layer new obligations on infrastructure actors for whom compliance is technically impractical and legally disproportionate under IPRED's own standards.

2. Conduct a prior assessment before blocking, in line with Articles 3 & 11 IPRED

The technical characteristics of shared Internet infrastructure make IP-based blocking inherently imprecise: a single IP address may represent thousands of servers and an even greater number of websites and services, meaning that blocking one address can render tens or hundreds of thousands of non-targeted domains unreachable. This risk is compounded when blocking obligations are extended to global DNS resolvers and VPN providers, which lack the technical means to apply geographically restricted blocks and are frequently neither based in nor subject to the jurisdiction of the issuing Member State - and which have no contractual relationship with the infringing content. EuroISPA submits that those outcomes are difficult to reconcile with the necessity and proportionality requirements embedded in Articles 3 and 11 of IPRED, which require that injunctions against intermediaries be strictly targeted and cause the least possible interference with lawful activity.

It is important, however, to distinguish between different categories of blocking measures, which are often conflated in practice. IP-based blocking is structurally prone to over-inclusion due to the shared nature of Internet infrastructure. Domain and DNS-based blocking rely on more specific addressing layers, but their practical precision depends on the quality of the underlying targeting data and the safeguards applied during execution, including validation and consistency checks. The policy challenge therefore relates less to the choice of technique per se and more to the robustness of the end-to-end implementation chain.

In addition, EuroISPA believes that national regulators should additionally be required to assess

blocking orders for compliance with Article 3(3) of the Open Internet Regulation (2015/2120) before implementation, not merely after the fact.

3. Give intermediaries sufficient and adequate time to assess blocking requests

EuroISPA proposes that enforcement timeframes should be calibrated to allow intermediaries -in particular micro, small, and medium-sized enterprises- sufficient time to conduct meaningful legality assessments consistent with the proportionality standard of Article 3(1) IPRED, ensuring that enforcement actions are accurate and targeted rather than precautionary and overbroad. The current absence of such mechanisms creates a structural burden that falls disproportionately on smaller providers, undermining both market competition and the proportionality requirements of Article 3 (2) of IPRED.

4. Make rightsholders accountable for overblocking

EuroISPA supports the position that rightsholders should be held accountable under Article 3(2) and Article 9 (7) of IPRED for collateral damage caused by overbroad blocking actions, with compensation mechanisms that are clearly defined and enforceable, ensuring that the burden of enforcement errors does not fall on innocent intermediaries and their users, consistent with IPRED's explicit prohibition on the abusive use of enforcement measures.

5. Create a space for industry cooperation

EuroISPA believes that collaborative approaches between stakeholders and national authorities built on direct engagement and the use of the disclosure and evidence-preservation mechanisms already available under Articles 6, 7, and 8 of IPRED are more likely to produce practical, sustainable, and proportionate outcomes than broad injunctive action against infrastructure layers. Such structured cooperation is better suited to addressing online piracy of live events than fragmented blocking obligations, particularly where enforcement requires coordination across multiple infrastructure layers such as IAPs, DNS providers, and hosting services.

6. Safeguarding fundamental rights in online blocking measures

Blocking measures rarely affect only their intended target. Because a single IP address may host thousands of unrelated services, orders aimed at unlawful streams routinely disrupt lawful speech, legitimate businesses, and access to information, as documented in the case studies below. This raises serious questions under the EU Charter of Fundamental Rights, in particular the freedom of expression and information (Article 11), the freedom to conduct a business (Article 16), and the right to an effective remedy (Article 47), especially where orders take effect before affected parties can be heard.

These concerns are reinforced by recent scholarship. A 2026 study by Quintais and Aznar finds that IP-based blocking causes structural overblocking, that extending measures to CDNs and VPNs is difficult to reconcile with the prohibition on general monitoring obligations under Article 15 of the e-Commerce Directive (2000/31/EC) and Article 8 of the DSA, and that the current drift toward private enforcement actors deciding what gets blocked - with limited transparency and no meaningful redress - amounts to an effective privatisation of enforcement that lacks adequate legal accountability.

Whether IP-based blocking can satisfy the CJEU's requirement of strict targeting is now directly at issue before the Court in Satel Film (Case C-400/24), with a ruling not expected before late 2026. EuroISPA urges the Commission to await that ruling before legislating in this area.

Ensuring a Future-Proof EU Copyright Framework amid Generative AI Developments

1. Maintaining the TDM exception

The TDM exceptions introduced by Articles 3 and 4 of the CDSM Directive represented a deliberate and forward-looking policy choice: to ensure that large-scale data analysis — the foundation of modern AI and machine learning — could take place in Europe without legal uncertainty. Since their transposition in 2021, these provisions have become critical infrastructure for a broad range of industries, including healthcare, cybersecurity, financial services, manufacturing, and education.

The emergence of generative AI has placed these provisions under renewed scrutiny. EuroISPA recognises the legitimate concerns of rightsholders regarding the use of copyrighted material in AI training. However, we caution strongly against any reform that would undermine the TDM framework based on an inadequately evidenced problem statement. The Commission's assessment must be grounded in demonstrated, concrete, and widespread harms — not assumptions or concerns that remain unevenly distributed across sectors and use cases.

2. Preserving voluntary opt-puts and interoperable technical standards

Where mechanisms relating to rights reservations are considered, their design should preserve flexibility and avoid introducing mandatory structural requirements that could fragment existing practices. EuroISPA believes that any centralised registry of opt-outs should remain voluntary in nature.

In addition, machine-readable expressions of rights reservations should be based on industry-

led and interoperable standards. This would support consistency and technical interoperability across systems while preserving adaptability across different stakeholders and use cases.

3. The need for an evidence-based problem definition

EuroISPA calls on the Commission to establish a clear, cross-sectoral evidence base before identifying or advancing any intervention options. The call for evidence, as currently framed, focuses primarily on potential impacts on rightsholders without sufficiently accounting for the wider ecosystem of data-driven industries that rely on TDM access. A proportionate review must address both sides of the ledger.

In particular, EuroISPA recommends the Commission to **gather evidence** on the following:

- **Demonstrable harm to rightsholders**: the scale, nature, and distribution of any adverse impacts, carefully distinguishing between AI training, fine-tuning, downstream commercial use, and general machine learning applications. Evidence must go beyond generative AI and consider the TDM regime's full operation since 2021.
- **Causal links:** whether identified harms are causally attributable to AI-related uses of content, or whether they reflect broader market, technological, or contractual shifts.
- **Costs of restriction**: how any proposed measures may affect data access, cross-sectoral innovation, and the availability of training inputs needed for AI development in the EU — including for the hosting, CDN, and data transit providers that are EuroISPA's members — and the risk of incentivising relocation of AI development outside Europe.

4. Preserving the effectiveness of the TDM exception

EuroISPA members -including hosting providers, CDN operators, and data transit services- have a direct interest in ensuring that TDM-related obligations are not extended to the infrastructure layer of the internet. EuroISPA is particularly concerned about proposals that would introduce new obligations or restrictions on intermediaries providing access to data, or that would expand the opt-out mechanism under Article 4 of the CDSM Directive in ways that fragment the information space available to AI developers operating within the EU. Such measures risk incentivising the relocation of AI development activity outside Europe and undermining the EU's stated ambition to lead in AI.

Any future intervention must be strictly proportionate, targeted at clearly evidenced and specific harms, and designed to preserve the effectiveness of Articles 3 and 4 of the CDSM Directive as enabling mechanisms for innovation across the economy.

5. Ensuring a proportionate allocation of responsibility in the AI value chain

EuroISPA believes that any EU approach to the relationship between AI and copyright should

preserve legal certainty and avoid fragmentation in the Single Market. A rebuttable presumption relating to the use of copyright-protected works should be limited to actors with direct control over the training and governance of general-purpose AI models. Downstream actors, including deployers and infrastructure providers, typically lack visibility over training datasets and should not be subject to evidentiary or compliance burdens. Regulatory responsibilities should therefore be allocated in line with the principle of proportionality and to the actors best placed to address the relevant risks.

Ensuring a common approach with the European Private Copying Exception

The EU's experience with the private copying exception illustrates the challenges that arise when Member States are afforded broad discretion in implementing copyright rules. Although the Copyright Directive and the case law of the Court of Justice of the European Union have established a common framework, significant divergences remain regarding both the scope of the exception and the design of compensation mechanisms.

The result has been a fragmented landscape, characterised by differing national remuneration schemes, varying legal interpretations, and inconsistent obligations across Member States. This legal and economic fragmentation creates complexity for businesses operating across borders and risks distorting competition within the Digital Single Market. These concerns were also reflected in the joint industry statement by EuroISPA, CISPE and the European DIGITAL SME Alliance on recent developments in Italy regarding private copying levies on cloud storage, which highlighted the risk of further regulatory divergence and Single Market fragmentation if Member States adopt uncoordinated approaches.

Conclusion

EuroISPA calls on the Commission to take full account of the concerns and recommendations set out in this submission. The review of the CDSM Directive presents an important opportunity to ensure that copyright law is fit for the digital age, but only if it is grounded in evidence, proportionality and genuine understanding of how the internet ecosystem works.

On piracy, EuroISPA believes that the answer is not more legislation, but better enforcement of what already exists. The Commission's own finding that the 2023 Recommendation had limited

effect should anchor this review. The IPRED framework, the InfoSoc Directive, the CDSM Directive, and the DSA together provide a substantial set of tools. What is needed is clearer calibration of those tools, stronger procedural safeguards, genuine accountability for overblocking, and structured cooperation between rightsholders and infrastructure providers.

Regarding generative AI, TDM exceptions must be preserved and clarified, not weakened based on assumptions. The EU's ambition to lead in AI depends on maintaining and enabling legal environments for data access and cross-sectoral innovation. EuroISPA urges the Commission to complete its evidence gathering before advancing any policy options.

Regarding the copyright levies, EuroISPA calls for greater EU-level harmonisation of the private copying exception, warning that diverging national implementations — such as Italy's cloud copyright storage levies - create legal complexity, distort competition, and fragment the Digital Single Market.

EuroISPA calls on the Commission to use the targeted legislative initiative as an opportunity to clarify and sharpen the existing framework, not to expand it or layer new obligations on actors who are structurally ill-placed to bear them.

Annex- Piracy Case studies

Italy: The Piracy Shield (introduced by Law n°93 of 2023) grants rightsholders the ability to direct the blocking of IP addresses and domain names within a 30-minute window, without judicial oversight or transparency. Private companies — not judges — decide what gets blocked, with no advance notice to affected parties and no mechanism for redress.

IP-level blocking has caused severe collateral damage. In February 2024, a Cloudflare IP block rendered tens of thousands of websites unavailable; in October 2024, an erroneous order took Google Drive offline for over 12 hours. Between February 2024 and June 2025, 7,742 domain names were impacted by collateral blocking — in one case, a single blocked IP disrupted 325 domains, while a Portuguese hosting provider suffered 16 days of lost email connectivity with Italian customers.

Rather than address these overblocking failures, AGCOM expanded the Piracy Shield's scope to DNS providers and VPNs — global services operating well beyond Italian jurisdiction. In March 2025, a Milan court ordered Google to block pirate websites through its public DNS servers. In September 2025, the University of Twente published the first peer-reviewed empirical study of the platform — *90th Minute: A First Look to Collateral Damages and Efficacy of the Italian Piracy Shield*, underlining how the indiscriminate IP-level blocking had disrupted hundreds of legitimate, non-streaming websites, including Ukrainian government educational and research sites and European NGOs

When Cloudflare refused to comply, AGCOM fined it €14 million, calculated on global revenue — nearly 100 times higher than what the company argues is the legal cap. Cloudflare appealed in March 2026.

Spain: LaLiga obtained a blocking order from Barcelona Commercial Court No. 6 in December 2024 allowing it to compel Spanish ISPs to block IP addresses linked to illegal streaming, without notifying cloud providers or disclosing to the court that the targeted IP addresses are shared infrastructure. The court upheld this ruling in March 2025, reinforcing LaLiga's authority — despite documented disruption to over 13,500 sites.

LaLiga has continued to interpret the order as a green light to unilaterally select IP addresses and domains to block, without ongoing court oversight. In February 2026, the Commercial Court of Córdoba granted an ex-parte injunction against NordVPN and ProtonVPN, issued based solely on LaLiga's arguments, without notifying the VPN providers or allowing them to present a defence. Since VPNs cannot selectively block one site behind a shared IP, they are forced to block large amounts of lawful traffic regularly.

Every weekend for the past year and a half, millions of Spanish internet users have lost access to banking apps, developer tools, and other platforms with no per-block judicial review and no mechanism for redress. Collateral damage has included Google Fonts, institutional sites, and payment platforms — all mistakenly blocked. This approach violates the principle of net neutrality, as also acknowledged by the Austrian regulator, which outlawed IP address blocking due to its associated over-blocking risks.

Austria: In August 2022, a rightsholder association requested Austrian ISPs to block a list of IP addresses linked to illegal music download sites. The blocks inadvertently made numerous legitimate websites — including online shops, news sites, and NGO websites — inaccessible, because the targeted IP addresses belonged to a shared content delivery network. As a direct consequence, the Austrian regulator outlawed IP address blocking due to its inherent over-blocking risks.

France: Following the first French court rulings involving VPN providers in May 2025, ARCOM demanded the blocking of 598 domain names from those providers. 81% of blocking requests sent to ISPs were also sent to alternative DNS services. The scope of enforcement is widening: the Paris Judicial Court in May 2025 ordered five major VPN services, NordVPN, ExpressVPN, Surfshark, ProtonVPN, and CyberGhost, to block access to 203 domains linked to illegal sports streaming. ARCOM is now pursuing an automated, real-time blocking system targeting live sports broadcasts, expected to be operational by mid-2026 raising concerns about the same overblocking risks seen elsewhere.

Belgium: the Belgium's court-led model — where a local court issues a blocking order and a dedicated government body oversees implementation — provides clearer procedural safeguards than in other Member States. However, the scope of obligations has grown. In April 2025, an order obtained by DAZN targeted not only ISPs but also third-party DNS resolvers

including Cloudflare, Google, and Cisco's OpenDNS, under threat of fines of €100,000 per day for non-compliance. Cisco pulled OpenDNS from Belgium entirely rather than comply, before the service was reactivated in July 2025 following a court suspension of the DNS blocking requirement pending appeal. The outcome of that appeal may have significant consequences for the scope of future blocking orders across the EU, as the trend of extending obligations to DNS resolvers and VPN providers continues to grow across Member States.

About EuroISPA

EuroISPA is recognised as the voice of the European Internet Services Providers industry, representing over 3,300 ISPs across the EU and EFTA countries.

Internet Service Providers (ISPs) include Internet Access Providers, Web Hosting Providers, Email Service Providers, Cloud Service Providers, Domain Registries and Registrars, Content Delivery Networks, Virtual Private Network Providers, Data Centres, Internet Exchanges and Online Platforms. ISPs also play a role in implementing Internet regulations and policies mandated by regulatory bodies like the European Union.For example, ISPs make it possible to timely detect and take down illegal content online and are a key partner of law enforcement authorities in promoting a safer Internet.

Contact: Rue de la Loi 38, 1000 Brussels | secretariat@euroispa.org | EU Transparency Register: 54437813115-56.