GIGAEurope Position Paper on the Digital Services Act

October 2021

GIGAEurope members welcome the efforts of the JURI committee to strengthen the Commission proposal on the Digital Services Act (DSA). We believe the DSA represents a watershed moment in the regulation of the digital sector which offers us a generational opportunity to update the regulatory framework for digital services in Europe.

Whilst the Opinion of the JURI committee aims to improve the Commission proposal, GIGAEurope members believe that several points/amendments need to be reconsidered in light of the core purpose of the DSA as well as the principles of necessity and proportionality. These provisions relate to: Article 5 (due diligence obligations for Hosting Service Providers), new Article 12a (General Risk Assessment and Mitigation Measures applicable to all intermediaries) and Article 13a (Online Interface Design).

In light of the upcoming vote on the IMCO Compromise Amendments we call on the committee members to oppose the amendments to Articles 5 and 12a adopted in the JURI Opinion. We believe that if the EU institutions get these provisions right, the legal framework can endure for the next decades, preventing national fragmentation, preserving fundamental rights whilst ensuring a safer digital environment for EU citizens.

Article 5: Obligations for Hosting Service Providers

We note that the JURI Opinion includes a requirement that "providers of hosting services shall, upon obtaining actual knowledge or awareness, remove or disable access to illegal content as soon as possible and in any event…within 30 minutes where the illegal content pertains to the broadcast of a live sports or entertainment event". In our view this is a concerning development, that threatens to undermine the DSA's core purposes as a harmonising piece of legislation, as well as endangering the fundamental rights of users.

- **Undermining the DSA's core purpose**: DSA is a horizontal legislation that addresses all types of illegal content pursuant to EU or Member States law. As such, provisions pertaining to the takedown of specific types of content (e.g. live sports pirated content, CSAM, copyright, terrorist content, etc.) should not be included in the DSA. Applying a stricter approach to live streaming sports events than other types of illegal material risks opening the door for the inclusion of other types of takedown deadlines for different types of sector-specific content in the DSA. Such an approach would therefore undermine the core purpose of the DSA to serve as a horizontal regime that harmonises EU rules for online intermediaries to tackle illegal and harmful material.

GIGA EUROPE
2-4 Rdpt. Schuman, 5th Floor • 1040 Brussels, Belgium • T: +32 (0) 2 521 17 63
office@gigaeurope.eu • www.gigaeurope.eu

- **Impact on the principles of necessity and proportionality**: Applying a horizontal requirement for **all hosting providers** to comply with the 30-minute deadline is not necessary nor proportionate. It would have an adverse impact on those service providers who do not materially contribute to the dissemination of illegal material online. Also, there's no objective justification for a two times stricter deadline as foreseen under the Terrorist Content Online Regulation, which includes a 1-hour takedown deadline, applicable only to services that **disseminate material to the public** – i.e. online platforms.

We therefore call on IMCO members to reject the strict take down time limits included in the JURI Committee Opinion, on the basis of the adverse impact such changes could have on EU citizen's fundamental rights, and harmonising aims of the DSA. At the very least, legislators should ensure that the provisions in the DSA are aligned with and do not go beyond those contained in the TCO (where one hour take down time limits apply for terrorist content, but only applicable to service providers that *disseminate material to the public*)[1].

Article 12a (new): General Risk Assessment and Mitigation Measures applicable to all intermediaries

We note that the JURI Opinion includes a general requirement that all intermediaries should carry out a risk assessment and put in place risk mitigation steps "related to the dissemination of illegal content through their services". It is the view of GIGAEurope members that such a requirement is ill conceived, impractical and necessary nor proportionate. Furthermore this new requirement departs from the Commission's original Impact Assessment for the DSA and abandons the risk based approach, which states as a general principle that service providers should only be subject to regulatory obligations that are proportionate to the risk posed by their services and that they have a practical possibility of implementing.

- **Intermediary services do not disseminate material to the public:** GIGAEurope members provide connectivity services that consist of the conveyance of packets of data across our secure networks from one end point to another. We are prohibited by law from either inspecting the contents of these electronic communications, and from blocking or throttling access to certain websites. As such, our members' core services do not in any way involve the dissemination of illegal material to the public, and as such, it would be impossible to comply with a risk assessment requirement based on this risk.

- Not only is such a requirement impractical, it also runs counter to the aims of the Digital Services Act as proposed by the European Commission: to clarify and update the legal framework for online intermediaries while targeting new obligations in a tiered approach at those service providers who pose the greatest risk (online platforms and Very Large Online Platforms).

[1] Article 3,3 of the Terrorist Content Online Regulation (2021/784)

We therefore call on IMCO members to return to these foundational principles of the DSA and reject the amendment in the JURI committee that would (without evidence or Impact Assessment) extend due diligence obligations explicitly targeted at the riskiest services in the Commission's draft to all intermediaries, regardless of the level of risk posed or impact on the service providers in question.

Article 13a: Online Interface Design

We note that the JURI Opinion includes new requirements for providers of intermediary services with respect to "the design, functioning or operation of online interfaces or a part thereof". As noted above, such provisions should only be targeted at service providers that pose a certain risk threshold, and who have the practical possibility to implement such requirement. Providers of **intermediary services that do not have an online interface** (for example: Internet Access, content delivery or caching) should **clearly not be subject to requirements relating to interface design.** Providers of hosting service that are passive in nature, and therefore do not manipulate, optimise or present content in a way which might be able to subvert or impair the autonomous decision making of the individual should also be excluded from such requirement, in line with the lower order of risk posed by their services. Therefore, we would support the introduction of online interface design requirements under Article 13a b**ut only if exclusively targeted at providers of online platforms or very large online platforms (VLOPs)** respecting the principles of proportionality and effectiveness.

***