

## Responsibility Online

### **Executive Summary**

Both politicians and internet companies need to do more to tackle illegal content online, and EDiMA and its members are ready to play their part.

As it stands, additional efforts to find and remove illegal content carry risks for internet companies. This system has created a perverse incentive whereby we are discouraged from taking action before being made aware of the existence of illegal content.

EDiMA envisages a new 'Online Responsibility Framework', that would enable and incentivise online service providers to do more to protect consumers from illegal content. Such a system can only work if online service providers know they won't be punished for taking additional measures, so limited liability must be reaffirmed as part of any new framework.

Illegal content is more clearly defined under national law than harmful content - this allows for speedy action on illegal content under this framework. Harmful content, on the other hand, is more complex and needs much broader consideration.

EDiMA and its members have unparalleled expertise in dealing with illegal content and are ready to offer that expertise to support legislators.

"Our members understand and share the concern that people have about illegal and harmful content online and we want to do more to tackle this problem. We need rules that allow us to take more responsibility online and these rules should encourage, not discourage further action" – Siada El Ramly, Director General of EDiMA.

### **What is the current problem?**

There is growing pressure on policymakers to bring forward proposals, particularly in the area of content moderation for illegal and harmful content. Under existing rules, internet companies are obliged to remove illegal content when they have been informed of its presence.

However, these rules also put internet companies at potential risk of losing their limited liability if they take measures beyond what's required by law. In this instance, companies can be reluctant to take additional measures, even if they might otherwise wish to do so.

### **What is the solution**

Given our role at the heart of the digital economy, EDiMA members can offer unique, first-hand insight into the evolving nature of technology and EU citizens' relation to it. We are eager to use our shared experience and insight to be a constructive driver of the "Digital Services Act" ("DSA") discussions in Brussels. While the implications of these discussions are likely to impact the wider online ecosystem including right holders, media, users, government and law enforcement, our solution is focused on the aspects of most relevance to our members. As an association bringing together various internet companies, we can inform policymakers as to what a potential new framework would look like in practice and what it would mean for European citizens.

There are a variety of aspects within these discussions that are of particular importance to our members. These include:

1. Objectives to be addressed
2. Distinguishing responsibility from liability

3. Workability with other initiatives
4. Scope of the framework
5. Content to be focused on
6. Potential oversight body

Each of these aspects are outlined in greater detail below.

## 1. Objectives to be addressed:

There are valid concerns about the abuse of online service providers to disseminate both illegal and harmful content online. In tackling these issues, it is essential to keep the benefits of the regime established by the e-Commerce Directive in mind, notably:

- The free movement of goods and services in the Internal Market has been made possible by the Country of Origin Principle, which allows companies to offer services across all Member States when established in one. This has boosted European businesses, cross-border trade and the uptake and growth of digital technologies.
- The provision of a sound legal basis for collaboration and contracting within complex digital supply chains.
- The promotion of innovation and the protection of third-party rights on the open internet made possible by the limited liability regime and the prohibition against a general monitoring obligation.

These foundational principles are more important today than they have ever been, as digital business models become more complex and an increasing number of players rely on the certainty they provide. In order to best address the concerns around illegal and harmful content, we believe that policymakers should consider a new complementary framework which builds on the existing law and reaffirms the limited liability regime and Internal Market principles, while clarifying roles and responsibilities online.

## 2. Distinguishing responsibility and liability:

EDiMA believes that a new framework should be created which clearly distinguishes between the principles of responsibility and liability.

The law should continue to assign primary liability to those users that act illegally or harm others and limit the liability of online service providers whose services are abused by others. The notice and action regime which accompanies the limited liability regime should remain the key set of rules governing specific illegalities – and in fact further clarity on notice and action rules would be welcome.

A new framework of responsibility could then set out roles and responsibilities for online service providers to tackle illegal content while respecting the unique features of the services. Responsibility in this sense would mean systemic steps, processes and procedures which a service provider can put in place to address illegal content or activity more proactively.

Under this framework, a service provider within the scope would then be in a position to take reasonable, proportionate and feasible actions to mitigate observed issues arising from the presence of illegal content or activity on their services. Service providers would define the kind of measures which best suit their unique situation, and which are the least intrusive for users.

Built-in safeguards would be required to ensure that measures taken under this framework of responsibility would not compromise service providers' limited liability. This would reconcile responsibility with online service providers' freedom to conduct a business, the need for legal certainty for both private sectors and competent authorities, and ensure that service providers are not perversely incentivised to interfere with their users' fundamental rights. To do so, it would be

important to retain the prohibition of a no-general-monitoring obligation, and the concepts of reasonableness, proportionality, and feasibility would need to be interpreted in a good faith manner by competent authorities and courts.

Ultimately, this new framework for responsibility would incentivise and give confidence to online service providers to take additional effective action against illegal content and activity on their services, in a manner that preserves the foundational legal principles of the open internet. This framework should also be complimented by analysis and action on the responsibilities that other actors in the online ecosystem can take to meet the objectives of tackling illegal content.

### 3. Workability with other initiatives:

While the structure of the initiative we describe should be a horizontal framework, applying to a variety of sectors or content, it could also incorporate or be complemented by sector or content specific rules based on the three pillars of policy – self-regulation, co-regulation and legislation.

In this way the new approach can co-exist with current rules and provide an overarching framework for responsibility online, while also making it possible to adapt quickly to address emerging concerns in the online space where there is concrete evidence that more specific vertical measures are needed.

### 4. Scope of the framework:

The scope of the new framework should be broadly defined, technology-neutral, and principles-based, applying proportionately to a variety of different online services rather than a specific list – which can become outdated or inapplicable in time. This is preferable to a patchwork approach which includes certain services in scope on the basis of criteria such as the size of the company or the type of content involved, as digital services are dynamic by design. The principles-based approach would establish a sliding scale of different measures that allows service providers to react appropriately to the concerns that are specific to their services and in a manner that is commensurate with their unique situations and abilities.

The concepts of proportionality and feasibility would then take account of situations where the nature of the service requires a different approach. For example, services such as electronic communications service providers and cloud infrastructure providers are more limited in what they can do to address illegal content uploaded or shared by their users, given the technical architecture of their services and the contractual relationships they hold with users. To expect the same content management efforts from their services as that requested of public-facing content sharing services belies their technical and operational nature, and would give rise to unjustified privacy, security, and commercial interferences.

### 5. Content to be focussed on:

To avoid fragmentation, the focus of a new framework should be precise and grounded on a solid legal basis which is readily applicable across all EU Member States. EDiMA therefore urges policymakers to focus on the management of illegal content and activity online as a starting point.

Illegal content is more easily defined and more consistent across the EU than content which is “harmful” but not illegal - the concept of “harmful” is subjective, depends greatly on context and can vary considerably between Member States when differences in culture and language are taken into consideration. The clearer definition of illegal content in national law would permit quicker action on tackling this content. Because the management of harmful content or activity requires nuance, a specific focus on the management of illegal content and activity at EU level will help to avoid infringing on fundamental rights for more context-specific cases.

That said, the focus on illegal content and activity in the new framework need not preclude further evaluation and action on “harmful” content. For example, self- and co-regulatory initiatives can be employed to build up best practices on these complex issues, with legislation to potentially be considered down the line where gaps are clearly identified.

## 6. Potential oversight body:

EDiMA accepts that a new approach might require some form of oversight to ensure it is effective for internet users, to which private actors and public authorities can also contribute. Should this element continue to be a part of the “DSA” conversation, we believe there are some key principles which should be kept in mind throughout the discussion.

Firstly, to honour the spirit of the e-Commerce Directive’s single market focus, an oversight body should be an EU-level body, or at the very least should function as an EU-level coordination mechanism for designated national authorities capable of delivering legal certainty and consistency for all parties.

Next, the benefit of an oversight body (whether new or an extension of an existing body) would be in their ability to provide guidance and oversight for service providers on adherence to their responsibility, and to ensure service providers are indeed taking reasonable, feasible, and proportionate measures. Crucially, the focus of an oversight body’s work should be restricted to the broad measures which service providers are taking – it should not have the power to assess the legality of individual pieces of content and it should not be empowered to issue takedown notices, which is the remit of the courts. Such competences call into play multiple critical constitutional and procedural questions, which are best left to the courts.

Finally, it should be co-regulatory in nature, such that there would be a clear consultative role for industry and civil society in its work. It would need to be staffed with technical and policy experts, to ensure the guidance and best practice it issues confirms to the spirit of the framework of responsibility. The potential oversight body should also borrow governance best-practices from existing oversight bodies in the tech sector and elsewhere – for instance, ENISA’s permanent stakeholder group, the concept of industry-driven codes of conduct overseen by data protection authorities, etc.

## **Conclusion**

The Commission’s “DSA” concept is an interesting starting point for discussions concerning content management and roles and responsibilities online. In these upcoming discussions it will be important to remember that no single actor alone can provide for an effective, scalable and transparent fight against illegal content and activity. Rather a complex network of businesses, individuals, NGOs, administrative or law enforcement agencies and online services need to work in concert towards shared public policy goals.

Past events have shown that we need to consider the online space as an ecosystem in which there are many different types of actors which disseminate content and enable activity in different ways – all of which bear some responsibility towards the preservation of a healthy online environment. Going forward, we urge policymakers to take the role of every actor in the online ecosystem into account and enforce their responsibilities effectively – be they users themselves, right holders, law enforcement agencies, trusted flaggers, etc.

Our members offer unique insight into the practicalities of attempting to address illegal and harmful content online. For that reason, we ask policymakers to consider the six aspects above and to engage with us and our members in the search for a solution that will work.