



EU Unpacked

euawareness.org

[#KnowledgeAgainstManipulation](https://twitter.com/KnowledgeAgainstManipulation)

EU Unpacked #11

George Robakidze

The EU Regulation on the Single Market for Digital Services

Understanding the EU's framework for the online environment

An In-Depth Analysis for Non-Experts

The opinions and conclusions expressed are those of the author and do not necessarily reflect the views of the EU Awareness Centre.

April 2026

© [2026] EU Awareness Centre. All rights reserved.

The EU Regulation on the Single Market for Digital Services

Understanding the EU's framework for the online environment

Part I – Why the Digital Services Act exists and what it regulates

A new rulebook for the digital public space

For more than two decades, the European Union has relied on a legal framework designed for a fundamentally different digital environment. When the E-Commerce Directive was adopted in 2000, online services were relatively simple: websites mainly provided static information, communication possibilities were limited, and e-commerce was still at an early stage of development.

Today, the digital environment has been fully transformed. Large digital platforms shape not only how users access information, but also how economic transactions take place and, increasingly, how public discourse is formed.

The role of these platforms changed significantly: they no longer operate merely as passive intermediaries. Instead, they actively curate, organise, recommend, and monetise content. These processes are often carried out through complex automated systems whose functioning is not fully transparent to either users or regulators.

The [Digital Services Act \(DSA\)](#) is the EU's response to this transformation. It focuses on **how digital power is exercised**, introducing rules on responsibility, transparency, and accountability in the online environment.

At its core, the DSA asks a fundamental question: *how can digital services operate at scale while remaining consistent with democratic values, fundamental rights, and the rule of law?*

Why did the EU decide to act?

By the end of the 2010s, it was obvious that the EU's legal framework no longer corresponded to the realities of the existing digital environment.

As the illegal content, unsafe products, scams, fake news and disinformation were spreading fast across Member States, enforcement mechanisms remained fragmented and inconsistent. National authorities struggled to take action against platforms based in other Member States, while the level of consumer protection varied significantly across the Union.

In response to this situation, individual Member States started to develop their own national regulations, mainly in areas such as content moderation and platform responsibility. Despite the fact that these initiatives addressed real, existing challenges, they also produced a significant side effect expressed in regulatory fragmentation.

This fragmentation had increased legal uncertainty for companies, particularly for those that operated across the European Union. By the late 2010s, it had become clear to all actors that the existing framework was no longer sufficient.

From the EU's point of view, this circumstance also posed a direct challenge to the **Single Market**, as the national laws were putting up barriers to digital services and cross-border activity, basically threatening one of the Union's core principles.

The DSA therefore pursues a dual objective:

- **to ensure a safe and trustworthy online environment, and**
- **to preserve the integrity of the Single Market through harmonised rules.**

What does the Digital Services Act do and does not do?

The DSA often is handled as a law about controlling online speech, which is not correct. In reality, it approaches the issue in a more structural and procedural manner. The Regulation **does not define what**

illegal content is, this remains the subject of other existing EU and national laws. Instead, the DSA is dealing with how platforms handle content and manage risks. In practice, it:

- sets clear steps for **management of illegal content**;
- makes platforms **more transparent**, including moderation and algorithms;
- gives **clearer rights to users** and opportunities to challenge decisions;
- **places extra responsibilities** on very large platforms;
- and puts in place a **coordinated system for enforcement** across the EU.

At the same time, the Regulation intentionally avoids turning platforms into public authorities or requiring them to make political judgments about the truth or the legitimacy. This reflects a careful balance between **effective regulation and the protection of freedom of expression**.

Which services are covered?

The DSA applies to so-called **intermediary services**—services that transmit, store, or organise information provided by users. These services form the infrastructure of today’s internet.

The Regulation distinguishes between several categories:

- Mere conduit services – for example, internet providers that pass data on without changing it;
- Caching services – services that temporarily store data to make things run more efficiently;
- Hosting services – services that store content uploaded by users;
- Online platforms – platforms that share content with the public or connect users with each other;
- Online marketplaces – platforms that allow users to buy from and sell to businesses;
- Online search engines – services that help users find and access information online.

This classification is central to the DSA’s logic. **Obligations increase with the level of control and societal impact**. A small hosting provider is not subject to the same requirements as a large social media platform or a major online marketplace.

A proportionate approach: protecting innovation while regulating power

One of the main ideas of DSA is **proportionality**. This means that many additional obligations do not apply to **micro and small enterprises**, which in its turn reflects the EU’s broader regulatory philosophy: rules should be adapted to capacity and risk. At the same time, the Regulation makes it clear that **very large platforms cannot benefit from such exemptions**, regardless of their formal classification. Their real influence, especially on information flows and markets, justifies such stricter oversight.

This differentiated approach allows the EU to regulate systemic risks without crushing innovation.

No general monitoring: a fundamental safeguard

Another essential point which was introduced by the DSA is the **prohibition of general monitoring obligations**. This is an important step for protecting the **freedom of expression**. The DSA do not oblige platforms to monitor all their user content constantly. This, in its turn, prevents private actors from becoming arbiters or censors of online speech.

However, the absence of an obligation to conduct permanent monitoring does not mean that platforms are exempt from responsibility. Once the platform is informed of illegal content—through customers or other means—it is required to act **promptly and responsibly**. The DSA therefore draws a clear line between:

- prohibited blanket monitoring, and
- targeted action based on concrete knowledge.

Transparency as a core regulatory tool

Transparency is at the heart of the DSA’s approach. All covered services must:

- publish clear and accessible **terms and conditions**;
- explain how **content moderation decisions** are taken;
- provide information on the use of **automated tools and algorithms**;
- issue **regular transparency reports**.

These obligations are not only designed to inform regulators. They also enable **public scrutiny** by researchers, journalists, and civil society.

In this sense, the DSA treats transparency as a form of governance—ensuring that digital power is exercised in a way that can be observed, questioned, and evaluated.

Orders from public authorities and the rule of law

The DSA also clarifies how platforms must respond to **orders from national authorities**.

When a judicial or administrative authority issues a legally valid order to remove illegal content or provide information, platforms are required to comply **without undue delay**. At the same time, the Regulation introduces safeguards to prevent abuse. Such orders must:

- be based on **clear legal grounds**;
- specify their **scope and purpose**;
- respect **fundamental rights**, including the right to an effective remedy;
- remain **proportionate in territorial scope**, particularly in cross-border situations.

This framework ensures that enforcement remains anchored in the **rule of law**, rather than arbitrary or politically motivated interventions.

From fragmentation to a coherent digital framework

Taken together, these elements illustrate the broader ambition of the Digital Services Act. It is not a single-issue regulation, but a **systemic framework** designed to:

- address the risks of the digital environment;
- clarify responsibilities across the online ecosystem;
- and ensure that the internal market for digital services functions effectively.

By shifting the focus from individual pieces of content to **structures, procedures, and accountability**, the DSA marks a transition from reactive regulation to a more **principled and forward-looking model of digital governance**.

Part II – How the Digital Services Act works in practice

From ad hoc moderation to structured procedures

In the time before the Digital Services Act, platforms mostly handled illegal content under their own internal rules. These rules varied significantly: some platforms acted quickly, others slowly. Some provided explanations, others did not. To users, moderation decisions felt unpredictable and confusing.

The DSA replaced this fragmented landscape with a **structured procedural framework**. At the core of its system are **notice-and-action mechanisms**. Platforms now have to offer users clear, easy-to-use tools for reporting illegal content. These tools need to be straightforward, accessible online, and designed so users aren't put off by unnecessary complexity.

Once a notice is submitted, platforms are required to:

- assess it **diligently and without undue delay**;
- base decisions on **clear and non-arbitrary criteria**;
- and provide **reasoned explanations** for their actions.

This obligation to give reasons represents a significant shift. Content moderation is no longer a purely internal process—it becomes subject to **procedural accountability**.

Trusted flaggers: expertise within the system

To improve efficiency and accuracy, the DSA introduces the concept of **trusted flaggers**.

These are entities—often specialised organisations or public bodies—with demonstrated expertise in identifying illegal content. Their role is not to decide, but to **signal high-quality notifications**.

Platforms must prioritise notices submitted by trusted flaggers. This does not mean automatic removal, but it ensures that such notices are processed **more rapidly and with particular attention**. The system serves two purposes:

- it reduces the burden of assessing large volumes of notifications;
- and it strengthens cooperation between platforms and actors with recognised expertise.

At the same time, safeguards exist to prevent misuse of this status, ensuring that prioritisation does not undermine fairness.

User rights and redress mechanisms

One of the most important innovations of the DSA is the recognition that **moderation decisions can significantly affect users' rights**.

Content removal, account suspension, or reduced visibility may impact not only expression, but also economic activity—particularly for journalists, creators, and small businesses.

To address this, the DSA introduces a multi-layered system of **user protection and redress**. Platforms must:

- provide **internal complaint-handling systems**;
- ensure decisions are reviewed in a **timely and non-discriminatory manner**;
- and include **human oversight**, especially where automated tools are used.

If users are not satisfied with the outcome, they may turn to **out-of-court dispute settlement bodies**, certified at the national level. These mechanisms offer a more accessible alternative to litigation.

Importantly, these procedures do not replace judicial remedies. Users retain the right to bring cases before courts, ensuring that **fundamental rights remain enforceable**.

Online marketplaces: strengthening consumer protection

The DSA introduces targeted obligations for **online marketplaces**, reflecting their growing role in digital commerce.

While these platforms have expanded consumer choice, they have also facilitated the sale of unsafe, counterfeit, or illegal products—often by traders who operate across borders and are difficult to identify. To address this, the Regulation requires marketplaces to:

- collect and verify **essential information about traders**;
- ensure that **mandatory consumer information** is clearly displayed;
- and act promptly when illegal products or services are identified.

In addition, when platforms become aware of illegal activity, they may be required to **inform affected consumers**, strengthening trust in digital transactions.

These measures do not turn platforms into full regulators of products. Rather, they introduce **traceability and transparency**, closing gaps that previously allowed harmful practices to persist.

Very large platforms: systemic responsibility

A defining feature of the DSA is its differentiated approach to scale.

Platforms and search engines reaching at least **45 million users in the EU** are designated as:

- **Very Large Online Platforms (VLOPs)**; or
- **Very Large Online Search Engines (VLOSEs)**.

These services play a structural role in shaping information flows, markets, and public discourse. As a result, the DSA imposes **additional obligations reflecting its systemic impact**.

The underlying logic is clear: **The greater the influence, the greater the responsibility**.

Addressing systemic risks

Unlike smaller services, very large platforms must go beyond individual cases and address **systemic risks** arising from how their systems operate. These risks include:

- the large-scale dissemination of illegal content;
- negative effects on **fundamental rights**;
- manipulation affecting **democratic processes**;
- risks to **public security and public health**.

Rather than prescribing fixed solutions, the DSA requires platforms to:

- identify and assess these risks;
- adopt **proportionate mitigation measures**;
- and continuously evaluate their effectiveness.

This approach shifts the focus from reactive moderation to **proactive risk governance**.

Independent audits and oversight

To ensure that these obligations are meaningful, very large platforms are subject to **independent annual audits**. These audits assess:

- compliance with DSA obligations;
- and the effectiveness of risk mitigation measures.

The objective is not only enforcement, but **accountability based on evidence**. Regulators and the public gain greater insight into how platforms operate, while companies are required to demonstrate—not merely claim—compliance.

Algorithms, recommender systems, and user choice

The DSA recognises the central role of **algorithms and recommender systems** in shaping the online experience.

Rather than restricting their use, the Regulation focuses on **transparency and user autonomy**.

Platforms must:

- explain the **main parameters** behind recommendations;
- clarify how content is prioritised;
- and provide explanations in **clear and accessible language**.

Crucially, users must be offered at least one option that is **not based on profiling**.

This requirement introduces an element of **choice and control**, reducing dependence on opaque optimisation systems and allowing users to engage with information on different terms.

Online advertising: from opacity to visibility

Online advertising is a core component of the digital economy, but it also raises concerns about manipulation, targeting, and a lack of transparency.

The DSA introduces stronger requirements, particularly for large platforms. Users must be able to identify clearly:

- when they are viewing an advertisement;
- **who is behind it;**
- and why it is being shown to them.

For very large platforms, this is complemented by **public advertising repositories**, which provide information on:

- advertisers;
- targeting criteria;
- and the duration of campaigns.

These tools enable **public scrutiny**, particularly in sensitive contexts such as elections or public policy debates.

Crisis response: flexibility in exceptional situations

The DSA includes a mechanism to address **extraordinary circumstances**, such as:

- armed conflicts;
- terrorist incidents;
- or major public health crises.

In such situations, the European Commission may activate a **crisis response framework** for very large platforms. These measures are: **temporary and targeted**, designed to address urgent risks and subject to safeguards to protect fundamental rights.

This is the clear reflection of the EU's approach to balance **regulatory flexibility with legal certainty**.

Enforcement: national authorities and EU coordination

The DSA establishes a **multi-level enforcement system**. Each Member State is obliged to designate a **Digital Services Coordinator**, responsible for supervision and enforcement of the Regulation at the national level.

These authorities cooperate across borders, ensuring consistent application of the rules.

However, for very large platforms, the **European Commission plays a central role**, reflecting their cross-border impact and systemic importance. This combination of national and EU-level oversight aims to ensure both **proximity to users and local contexts** and **consistency across the Single Market**.

Sanctions and incentives for compliance

To ensure effectiveness, the DSA provides enforcement authorities with a range of tools, including:

- **finances;**
- **periodic penalty payments and corrective measures.**

EU sanctions are designed in such a manner that they are both **proportionate and hindering**. This approach ensures that compliance is not optional. At the same time, the framework encourages **dialogue and corrective action**, recognising that regulating complex digital systems requires continuous engagement rather than one-off interventions.

The Digital Services Act in practice

Taken together, these mechanisms illustrate how the DSA operates as a **comprehensive governance framework**. It moves beyond isolated measures and establishes clear procedures, defined responsibilities, enforceable rights and structured oversight.

For users, this means greater transparency and stronger protections. For businesses, it provides clearer rules and legal certainty.

For policymakers, it offers tools to address systemic risks without undermining innovation.

The DSA does not eliminate all challenges of the digital environment. But it is definitely a big step towards a model in which digital power is exercised within a framework that emphasises accountability, transparency, and democratic oversight.

Part III – Implications, challenges, and strategic outlook

A new model of digital governance

With the Digital Services Act, the European Union moves beyond ad hoc responses to online harms and establishes a **systemic governance framework** for the digital space.

The Regulation reflects a broader shift in EU policymaking: from reacting to individual crises to structuring the exercise of digital power. Instead of focusing solely on content, the DSA targets the **systems, incentives, and procedures** through which content is created, distributed, and amplified.

In this sense, the DSA is not just a technical instrument—it is part of the EU’s wider ambition to shape the **rules of the digital public sphere**.

Balancing regulation and fundamental rights

A central strength of the DSA lies in its attempt to balance two competing imperatives:

- the need to address illegal content and systemic risks;
- the obligation to protect **freedom of expression and other fundamental rights**.

By prohibiting general monitoring and avoiding direct regulation of speech, the EU seeks to prevent platforms from becoming private censors. At the same time, procedural obligations—such as notice-and-action systems and transparency requirements—ensure that platforms cannot avoid responsibility.

However, this balance remains fragile.

In practice, platforms may still adopt **risk-averse moderation strategies**, potentially leading to over-removal of lawful content. The effectiveness of the DSA will therefore depend not only on legal rules, but also on **how those rules are implemented and enforced**.

From platform neutrality to platform responsibility

The DSA marks a clear departure from the earlier idea of platforms as **neutral intermediaries**.

While the Regulation preserves liability exemptions, it introduces a layered system of **due diligence obligations**, recognising that platforms actively shape digital environments. In particular, very large platforms are expected to assess and mitigate systemic risks linked to their design choices.

This shift reflects a broader understanding: **Digital infrastructures are no longer passive channels, but actors with societal impact**.

At the same time, the EU stops short of treating platforms as public authorities. The DSA does not require them to determine what is “true” or “legitimate”, but rather to operate within a framework of accountability.

Enforcement: the real test of the DSA

As with many EU regulations, the success of the DSA will depend heavily on **enforcement**. The framework relies on a combination of:

- national Digital Services Coordinators;
- cross-border cooperation mechanisms;
- and a central role for the European Commission in supervising very large platforms.

This multi-level system reflects the structure of the Union, but it also introduces challenges:

- differences in administrative capacity across Member States;
- potential inconsistencies in interpretation;
- and the complexity of overseeing global digital actors.

Ensuring **effective and consistent enforcement** will be critical to maintaining both credibility and legal certainty.

Global implications: the “Brussels effect” in digital regulation

The DSA is likely to have an impact beyond the European Union.

Given the size of the EU market, many global platforms may choose to apply DSA standards more broadly rather than operate multiple regulatory systems. This phenomenon—often referred to as the “**Brussels effect**”—positions the EU as a global standard-setter in digital governance.

At the same time, the EU model differs from approaches taken elsewhere:

- it is more rights-based than purely market-driven systems;
- and less state-controlled than more centralised regulatory models.

This positions the DSA as a **distinct regulatory model**, combining market integration with democratic safeguards.

Relevance for EU-aspiring countries

For countries seeking closer integration with the European Union, including those in Eastern Europe and the South Caucasus, the DSA has important implications.

Alignment with EU digital standards is likely to become part of broader **regulatory convergence processes**, particularly in areas such as:

- platform governance;
- consumer protection;
- and the fight against disinformation.

At the same time, implementation may be challenging. The DSA requires:

- institutional capacity;
- independent regulatory authorities;
- and a legal culture grounded in **fundamental rights and rule of law principles**.

For these countries, the DSA is not only a regulatory framework but also a **benchmark for democratic digital governance**.

Limits and open questions

Despite its ambition, the DSA does not resolve all challenges of the digital environment.

Several questions remain open:

- How effectively can systemic risks be measured and mitigated in practice?
- Will transparency obligations translate into meaningful public oversight?
- Can regulators keep pace with rapidly evolving technologies, including AI-driven systems?
- And will enforcement remain consistent across the Union?

Moreover, the DSA operates alongside other major EU instruments, creating an increasingly complex regulatory landscape that may be difficult for smaller actors to navigate.

Conclusion: a structural shift in EU digital policy

Taken together, the Digital Services Act represents a **structural shift** in how the European Union approaches the digital space.

It moves beyond a model of minimal intervention and establishes a framework based on:

- **accountability,**
- **transparency,**
- and **proportionate responsibility.**

The DSA does not eliminate all risks associated with digital platforms. However, it sets clear expectations for how those risks should be managed and how digital power should be exercised.

In doing so, it contributes to a broader objective: **ensuring that the digital environment remains compatible with democratic values, fundamental rights, and the principles of the European project.**

April 2026



George Robakidze

George is a diplomat and expert in international politics, security and European integration. During his career in the Georgian public service (2004–2023), he held senior positions focused on political affairs, European and Euro-Atlantic integration and regional security. Beyond diplomacy, he has contributed extensively as an author and researcher, specialising in the rise of radical and populist movements in Eastern Europe. He currently serves as the executive director of the EU Awareness Centre, a Brussels-based NGO promoting democratic reforms, good governance, and EU values. He continues his work as an independent researcher on political and international issues.