GENERAL REPORT

TOPIC II – EU Digital Economy: general framework (DSA/DMA) and specialised regimes

*Martin Husovec**

Table of Contents

* Associate Professor at the London School of Economics and Political Science. Disclosure: Dr Martin Husovec acts as a counsel for three non-profit organisations appearing as interveners on the side of the European Commission in the following pending DSA/DMA cases: *Zalando v Commission* (T-348/a23), *Apple v Commission* (T-1080/23), *Technius v Commission* (T-134/24). He also provided educational training on the EU Digital Services Act to staff of all regulators in the European Union, including the European Commission, technology companies, non-profit organisations, auditors, consultancies, and law firms.

Section 1: Introduction

This report has been prepared with tremendous help from many individuals. First, I would like to thank all the national rapporteurs who have contributed with their national reports as well as institutional rapporteurs who also helped me to draft the original questionnaire. Readers can read the extensive national and institutional reports in full at the end of this document. The report covers the period until 20.3.2025.

Second, I would like to acknowledge the help of two national rapporteurs who helped me draft the general report. Inge Graef and Alexander de Streel have generously contributed their ideas and drafting to the DMA section of this report. I also wish to thank many other experts who have spoken to me in the last two years. Many of my observations are based on numerous discussions with various stakeholders and experts. Mistakes and omissions, as always, are solely mine.

Finally, I would like to thank Marianne Bellavance who masterfully prepared the comparison section of this report and without whose help I would have grown much more grey hair. I hope the readers will find this report helpful when thinking about the future of the Digital Services Act and Digital Markets Act.

A regulatory moment

One popular narrative around digital services is that they flourished thanks to the absence of state regulation. The narrative is hardly accurate. The great majority of today's popular digital services, such as social media, marketplaces, video-sharing services, or app stores, were largely *enabled* by the early legislation in many countries. In the absence of this legislation, there was a real prospect that the vibrant internet as we know it today would not emerge due to excessive liability rules that would inevitably suppress people's ability to communicate with others without editors. The legislation saved companies years of litigating generalist rules and shaped how related areas of law thought about the issue.

In the United States, Section 230 of the Communication Decency Act (CDA) and Section 512 of the Digital Millennium Copyright Act (DMCA) made the provision of user-generated content services possible because they rejected potential strict (editorial) liability of new intermediaries for their users' content.[1]

Similarly, in the EU, of which the UK was part at the time, Section 4 of the E-Commerce Directive,[2] inspired by the DMCA, rejected potential strict liability

[1] Communications Decency Act of 1996, 47 USC § 230 (1996); Digital Millennium Copyright Act of 1998, 17 USC § 512 (1998).

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

for non-editorial user-generated content and thus provided a protective legislative shield across the EU Member States. The European legislation was unprecedented in its reach, cutting through the entire legal system, to protect intermediaries from potential strict liability.

Without such affordances, the digital services that we know today could not have emerged in the same way.[3] Their legal liability across the European legal system would have been much more complicated and thus costly. Any potential harsh negligence or strict liability standards would have pushed companies to a more editorial-style relationship with user-generated content and thus turned the ecosystem into a fancy television.

This is why not only legislatures but also the highest courts were rightly highly critical of it.[4] Decentralised non-editorial expressions of citizens unlocked unprecedented value for societies around the world, and increased participation of masses in the public spaces.

It is remarkable that when the early legislation was adopted, most Europeans and Americans did not have access to the internet.[5] With the majority of the population offline, it was harder to imagine the problems that non-editorial content would cause, especially if coupled with sophisticated algorithmic recommender systems, and attention-focused business models. Twenty years later, the problems associated with non-editorial content have crystallised well enough, although the evidence on the structural causes is sometimes still thin. Thus, reacting to challenges in nuanced ways remains a work in progress. However, the legislatures in Europe could no longer ignore the various societal crises that play out very significantly online.

Confronting these societal problems was not made easier by the fact that most of the solutions require the cooperation of new providers of digital services, and most of the biggest digital services are provided by US companies that have often grown into economic powerhouses. Many EU states, and their authorities, before the adoption of EU-wide rules of second generation (DSA/DMA), struggled to enforce their own laws in their own states. Laws like the Digital Services Act are thus partly born out of the frustration with this situation where foreign companies do not have sufficient commercial or political incentives to cooperate. The Digital Markets Act, in contrast, came out of the frustration of European businesses with their new business partners who had

[3] Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell UP 2019); Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Tech LJ 3.

[4] See *Reno v. ACLU*, 521 U.S. 844 (1997); *Delfi AS v. Estonia*, App. No. 64669/09 (Jun. 16, 2015), *Magyar Jeti ZRT v. Hungary* App. No. 11257/16 (Dec. 4, 2018), *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* App. No. 22947/13 (Feb. 2, 2016); *Sanchez v. France* App. No. 45581/15, (Sept. 2, 2021); Case C-401/19, *Poland v. Council & Eur. Parliament* [2021] ECLI:EU:C:2021:613.

[5] Martin Husovec, *Principles of the Digital Services Act* (OUP 2024), 57 ff.

unmatched market power over their digital ecosystems and could coerce them into one-sided technical, organisational and commercial arrangements.

The domination of one country as an exporter in any sector cannot stop legislatures in the receiving markets from regulating imported products and services. Otherwise, legislatures in these countries would abdicate the mandate from their constituencies. Introducing rules on safety and fairness is not any different. If German cars are very popular in Canada, they must be adjusted to local requirements for safety, interoperability, and commercial practices. Even though some equate such regulation immediately with protectionism, as I will show, this is hardly convincing in the case of the DSA/DMA. Foreign tech companies are tremendous beneficiaries of the harmonised EU legislation, and various mechanisms introduced by these two laws.

If the tech companies do not want to offer the obligatory features in other jurisdictions, they are free to do so. Again, this is nothing special. If for instance, the EU imposes seat belts for its market, cars sold in other markets do not have to be designed the same way. The early DSA/DMA compliance shows that tech companies are largely localising European compliance.

Goals of the DSA/DMA

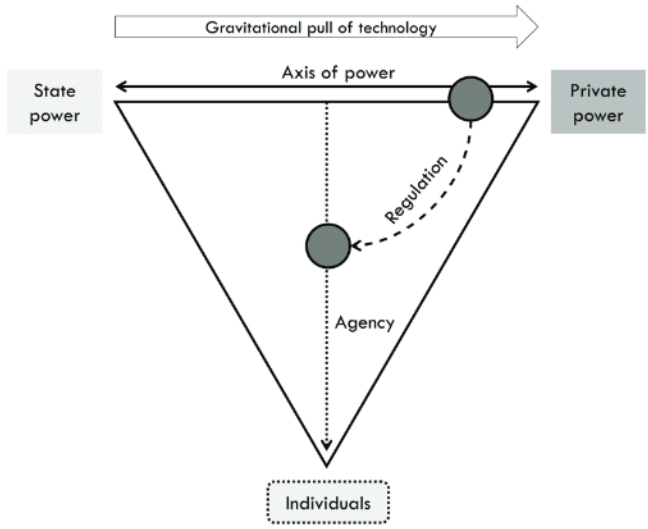
The Digital Services Act (DSA) and the Digital Markets Act (DMA) were adopted in late 2022 with the goal of regulating digital services.

The DSA aims to safeguard "safe, predictable and trusted online environment," while the DMA 'contestable and fair markets in digital sector'. Despite the different focus, their combination is more than logical. Both laws redistribute power from the tech companies to their customers, that is, users, albeit in different ways and for different purposes.

The DSA intervenes to redistribute the power that tech companies exert over users' speech and online experience to increase people's agency, sense of safety, and freedom. The DMA intervenes to redistribute the tech companies' power over their products to create more space for innovation by business users. While the DMA tries to diffuse the market power of big tech companies ("gatekeepers"), the DSA creates minimum regulatory requirements that must be met by all market entrants. Even though bigness is considered for the purposes of the DSA too, it mostly serves to avoid over-regulating micro, small and medium-sized enterprises.[6] The most onerous rules apply to digital services with 45 million monthly active users in the EU ("VLOPs" or "VLOSEs").

[6] Once the threshold of 45 million EU users is reached, the size of the company is irrelevant (see Article 19(2)).

Figure 1. The Empowerment Rationale



Source: Husovec, 2024[7]

The DSA/DMA end the period of little to no specific regulation of digital services. Obviously, these services have been subject to the GDPR but data protection only regulates one aspect, and is more horizontal law. In this case, the envisaged redistribution of power takes the form of sector-specific legislation, more specifically an EU regulation. Fairness in the DMA is about giving business users enough space to develop their businesses via the established digital ecosystems. Fairness in the DSA is about how users – consumers and businesses – experience the design and content moderation processes of digital services.

The Member States, through the European Union, are putting their thumbs on the scales of online safety and innovation to achieve all this together. Inevitably, the Member States collectively and individually assume new powers of their own to supervise digital services. This dynamic is not very surprising given that the prior experience of 20 years made a perfect case for a need of harmonised rules. Especially in small and mid-sized Member States it was often felt that tech companies had very weak political and economic incentives to pay attention to their local problems. Thus, along with individuals and business users that are potentially emerging stronger from the adoption of the DSA and DMA, so are the Member States themselves.

The common denominator of the DSA/DMA is **user empowerment**. Both regulations send an identical message to companies. European citizens do not wish to uncritically and without reservation accept any digital technology as

[7] Martin Husovec, Principles of the Digital Services Act (OUP 2024), Chapter 1.

designed by a few companies that are motivated mostly by quick profits or their own ideologies. Through their representatives, European users oblige tech companies to introduce adjustments to their services and ways of doing business that better reflect also other interests that they, the customers, hold dear.

European businesses and consumers are gaining new ways to control their online experience on digital services. If the DSA/DMA succeed, businesses and consumers gain the ability to do business online and understand the providers' decision-making, more easily switch between competing services, run apps otherwise restricted by app stores, customise their recommender systems on social media, contest termination of their accounts on online platforms, or personalise their interactions on social media to better reflect their safety preferences.

The Member States, in contrast, gain the ability to better enforce their regular laws about what is prohibited to say or do online from their territory. The DSA is thus **an extra regulatory layer** that grants the state authorities, individuals and civil society new paths to enforcement of what parliaments establish to be illegal. States thus remain in charge of authoritatively regulating content, and the behaviour of users, but the platforms now have a clearer list of expectations through which such content laws are enforced. For instance, the platforms must have processes for illegal content notification, encourage professional notifiers ("trusted flaggers") to send them as many notifications as they find, adjust the design of their services to factor in also the safety of users, or objective vulnerabilities.

These adjustments are meant to increase the **trust of users** in the decision-making of online platforms. Paradoxically, even the second Trump administration, a great critic of the DSA, is asking the tech companies a similar set of questions in the United States. The recent investigations of the US Federal Trade Commission to unearth "censorship" by tech companies sent a set of questions that closely resemble the due process requirements of the DSA, such as demanding an explanation of their practices, their consistency appeals mechanisms, etc.[8] It seems that if the questions are sent by the right agency, these demands are not that censorial after all.

Regulation: costs and benefits

While new regulations are resented by some as potential "over-regulation," both the DSA and DMA have underappreciated effects of lowering the barriers to entry to the EU markets. The reduction of barriers to entry is especially important for the DSA which harmonises a broad range of rules. While the scope of harmonisation by the DMA is not as broad, its substantive rules help the entry of business users that use gatekeepers' services.

[8] The Federal Trade Commission, ‚Request for Public Comment Regarding Technology Platform Censorship' (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/P251203CensorshipRFI.pdf

Prior to the DSA, all Member States were at liberty to regulate digital services as they saw fit, with some limits imposed by the liability regime, the country-of-origin principle and EU primary law. This means that companies had to face 27 national laws, possibly also additional regional laws, and, potentially deal with over a hundred responsible authorities. Moreover, companies without an establishment in the EU did not even benefit from the country-of-origin principle.[9]

Since the DSA, all companies around the world that wish to enter the European market have a firm and fully harmonised rulebook that mostly does not tolerate national deviation.

Thus, while the fact of being regulated is clearly an extra cost for companies, the opportunity of being regulated so *uniformly* is a tremendous benefit, especially for small and medium-sized companies anywhere in the world. Even though the DMA does not have as broad pre-emptive effects as the DSA, it still replaces deviating national rules across the EU, concentrates enforcement, thus avoiding fragmentation, and opens the opportunities for innovation by business users from anywhere in the world, not just by those from the EU.

According to some, the DMA/DSA are plots to extract revenues from US tech companies. As explained by FCC Chair, Brendan Carr: "If there is an urge in Europe to engage in protectionist regulations, to give disparate treatment to U.S. technology companies, the Trump administration has been clear that we are going to speak up and defend the interests of U.S. businesses."[10] Put differently, some think that "the DSA and DMA were never really principled actions, but rather an effort to create a new industry of compliance and to generate revenue based on fines."[11] If that were the case, the instruments have been poorly designed because extracting high fines is not that simple for the Commission (see below).

The benefits of the DSA/DMA are open to anyone operating in the EU markets, including foreign companies. They also pre-empt a much more complicated web of national rules. The American criticism incoherently lambasts the law as "targeting US companies" and "helping Chinese companies."[12] This refrain is something that some US representatives repeatedly tend to use in other markets that seek to regulate their companies (e.g., South Korea).[13]

---

[9] E-Commerce Directive (n 3), art. 3.

[10] Reuters, 'US FCC chair says EU Digital Services Act is threat to free speech' (3 March 2025), https://www.reuters.com/technology/eu-content-law-incompatible-with-us-free-speech-tradition-says-fccs-carr-2025-03-03/

[11] Dean Jackson and Berin Skóza, 'The Far Right's War on Content Moderation Comes to Europe' (11 February 2025), https://www.techpolicy.press/the-far-rights-war-on-content-moderation-comes-to-europe/ (quoting Kate Klonick who reports what some people in the industry think).

[12] Reuters, 'US demands EU antitrust chief clarify rules reining in Big Tech' (23 February 2025) https://www.reuters.com/technology/us-demands-eu-antitrust-chief-clarify-rules-reining-big-tech-2025-02-23/

[13] See for instance Lilla Nóra Kiss, 'Why South Korea Should Resist New Digital Platform laws' (*Information Technology & Innovation* Foundation December 2024), https://itif.org/publica-

Already for the reasons stated above the claims that the two laws are protectionist in spirit are hardly convincing. The fact alone that regulatees are often US companies only reflects the market success of these services and mostly applies to several product categories. Under the DSA, very large online platforms (VLOPs) are predominantly US companies in the segment of social media and app stores, but exclusively EU companies in the segment of adult sites. Marketplaces, in contrast, are represented equally by US, Chinese and European companies. Moreover, the DSA outside of the VLOP/VLOSE category predominantly regulates local European companies. Their numbers are in the thousands.[14]

Under the DSA, access to data is open to all researchers around the world if they study effects in the EU. Under the DMA, any company take advantage of interoperability provisions to offer their services in Europe. There are no rules that specifically favour European companies either as providers or as users. Even the requirement of "legal representative" under the DSA in fact helps the foreign companies without establishment because they can pick one EU regulator instead of facing 27 of them for a few thousand euros a year (see Article 56(7)). As demonstrated by the stakeholder engagement to date, the DSA and DMA managed to engage a global ecosystem of players, including many foreign companies and researchers.

Because the DMA only applies to bigger players, it has arguably little direct negative effect on new market entrants. Such effects could theoretically take place were the DMA to strip gatekeepers of substantial abilities of appropriation of their investment, which is hardly the case. The DMA rather marginally *calibrates* the ability of companies to appropriate their investments. It puts some limits on how they can exploit their ecosystems in the pursuit of profit by giving some affordances to users and banning some practices.

The DSA, in contrast, applies to all businesses; however, it staggers the set of obligations and doses them based on the size. Micro and small companies are subject to more limited rules. Only mid-sized companies are regulated as platforms. Yet, as will be argued below, there are still some obligations for micro and small companies that might be not properly calibrated for the size and role of these companies. Finally, only companies with more than 45 million monthly active users in the EU are subject to the most onerous obligations as very large online platforms (VLOPs) or very large online search engines (VLOSEs).

---

tions/2024/12/09/south-korea-should-resist-new-digital-platform-laws/

[14] Carl J. N. Frielinghaus et al., 'Zur Ausschreibung: „Studie zur Umsetzung des Digital Services Act in Deutschland - Bestandsaufnahme der relevanten Akteure"' (2024). https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/DSA/studie_dsa_akteure.pdf?__blob=publicationFile&v=3

Institutional setup

The lessons from the enforcement of the EU data protection regime undoubtedly shaped the institutional set-up of the DMA and DSA. In the DMA, the European Commission has always exclusive competence. In the DSA, the European Commission has become the most powerful enforcer of the law against VLOPs and VLOSEs. The Commission is exclusively competent to supervise key parts of the DSA. While it can share its competence with the national authorities ("Digital Services Coordinators") in whose territory the platforms are established or legally represented,[15] the Commission has a priority and can always "relieve" DSCs of their competence.[16]

Thus, the Commission is the key regulator for the VLOPs/VLOSEs. However, for the remainder of the digital ecosystem, DSCs remain exclusively competent. This creates a unique situation where most micro, small and mid-sized companies, as well as some types of services, such as infrastructure services, are exclusively supervised on the national level. DSCs thus have a critical role in presenting the SME viewpoint when interpreting the DSA, because the Commission's work exclusively focuses on very large services.

From a broader perspective, the Commission has several roles. It supervises the implementation of the law by the Member States, it supervises some regulatees, and finally, it cooperates with the national authorities. Since both the DSA and DMA can and will be privately enforced, the Commission moreover is in a relationship with national courts that sometimes can hear cases running in parallel to their investigations. Finally, the Commission also is the ultimate guarantor of the consistency of the EU rules, and thus also supervises that the Member States' legislatures do not adopt legislation that would be pre-empted by the DSA and the DMA. In that sense, the Commission is sometimes helping companies, and sometimes enforcing against them; it is mostly cooperating with the Member States but sometimes also enforcing against them.

To complicate matters further, the Commission is also a political body that negotiates trade agreements around the world. This complicates matters because the Commissioner responsible for the DSA/DMA is also a member of the College of Commissioners that approves collective political decisions of the Commission. As politicians, these Commissioners could see the DSA/DMA compliance as a negotiation tool with external trading partners, or in the EU or national politics. Moreover, employees managed by such Commissioners might become worried about the political repercussions that their enforcement decisions could lead to.

[15] See Digital Services Act, art. 13.

[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), O.J. (L 277) 1 EU, art. 66(2).

The closeness of the DSA/DMA enforcement to politics is highly problematic for the credibility of the system. Thierry Breton's tenure as a responsible Commissioner has shown that over-motivated politicians who try to instrumentalise the law can do a lot of damage. The current attempts of the second Trump administration, which is openly and uncritically championing the US tech companies' maximalist interests, show that if you politicise the enforcement, there will be equally political backlash. I argue below that the system therefore must institutionally change to gain more distance from politics.

At the time of writing, the US government is actively and aggressively pushing against the DSA/DMA. The US Vice-President, JD Vance, even suggested that the US should not support European countries through NATO if the EU does not respect US freedom of speech.[17]

In my view, we must learn from the data protection law, where the Commission consistently negotiated weaker data transfer safeguards with the United States, than the ones that were expected by the Court of Justice of the European Union.[18] If we are serious about the empowerment of users in Europe, we must further insulate the DSA/DMA enforcement from the external and internal political pressures and create a dedicated and independent EU agency for this purpose.

Scope of regulations

The DMA and DSA target digital services. The DMA is a law for big companies, while the DSA is a law for small and big companies, with different rules for each of them. In the DSA, the big companies correspond to the so-called very large online platforms (VLOPs), and very large search engines (VLOSEs). In the DMA, they are so-called gatekeepers.

The DMA has a much more circumscribed scope. The law exhaustively lists several "core platform services" whose providers can be designated as gatekeepers. The DSA in contrast, relies on five broad categories to define its scope, namely "mere conduit," "caching," "hosting," "online platform," and "search engines."

---

[17] The Independent, 'JD Vance says US could drop support for NATO if Europe tries to regulate Elon Musk's platforms' (17 September 2024), https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html

[18] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559; Orla Lynskey, 'Digital Empire or Digital Fiefdoms? Institutional Tensions and the EU Right to Data Protection' Cambridge Yearbook of European Legal Studies (forthcoming).

Figure 2. Big Players under the DSA and the DMA

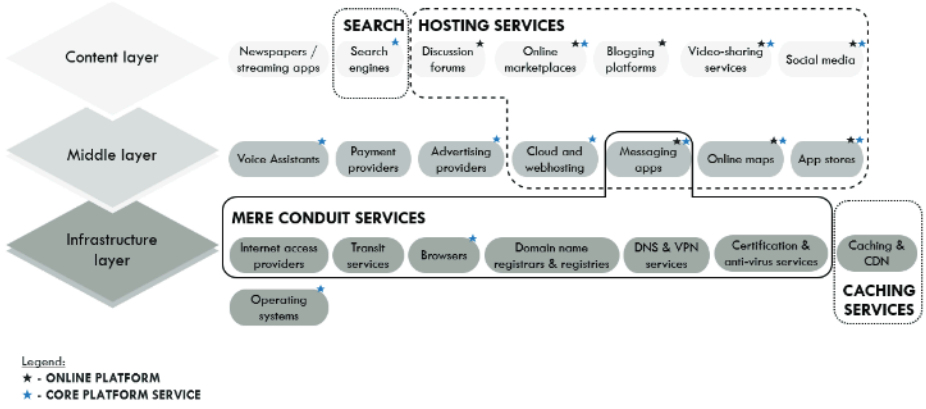
DSA		DMA	
Company	VLOP/VLOSE	Gatekeeper	CPS
Amazon	Amazon Store	Amazon	Amazon Marketplace
Alibaba	AliExpress		Amazon Advertising
Apple	Apple App Store	Apple	App Store
Alphabet	Google App Store		iOS
	Google Maps		Safari
	Google Shopping		iPodOS
	Google Play	Alphabet	Google Play
	Youtube		Google Maps
	Google Search		Google Shopping
Aylo Freesites	Pornhub		Google Search
Booking.com	Booking.com		YouTube
Bytedance	TikTok		Android Mobile
Infinite Styles	Shein		Google Advertising
Meta Mircosoft	Facebook		Google Chrome
	Instagram	Booking	Booking
Microsoft	LinkedIn	Bytedance	TikTok
	Bing	Meta Booking Bytedance Meta	Facebook Marketplace
NKL Associates	XNXX		Facebook
Pinterest	Pinterest		Instagram
Snap	Snapchat		WhatsApp
Technius	Stripchat		Messenger
Twitter	X/Twitter		Meta Ads
Webgroup Czech Republic	XVideos	Microsoft	LinkedIn
Wikimedia	Wikipedia		Windows OS
Whaleco Technology	Temu		
Zalando	Zalando		

Source: Own research

While for both laws it is a challenge to delimit the exact scope of services, under the DSA, the task can be incredibly complex. Especially the term "online platform" might require further elaboration, or at least clarification by means of examples in future legislation. In the DSA, the key problem is to separate what is regulated from what is not, especially if services have editorial and non-editorial content along with each other (e.g., podcasts and music, or maps and user reviews). In the DMA, the key challenge is the delineation of what is a Core Platforms Services (CPS), and what if one digital service includes several CPS services, some of which are big enough, and others that are not (e.g., social media, and its advertising, messaging parts).

In terms of coverage, both DMA and DSA cover large parts of the digital ecosystem, ranging from the *application layer* (social media, video-sharing services, marketplaces), *distribution layer* (search, cloud computing, advertising services, messaging services) to the *infrastructure layer* (browsers).[19] While the DSA never covers as big the services in the infrastructure layer because they cannot qualify as online platforms or search engines, the DMA covers big services across all three layers.

Figure 3. Regulatory Coverage of the Digital Ecosystem



Source: Own research

Even sidestepping the question of size thresholds, the DSA regulates many application layer services, such as dating, review, gaming, adult content, etc. This is especially true because what the DSA understands as a regulated service can constitute only a feature or subpart of an overall product (e.g., the comments section in newspapers, or hosting of event profiles for a live streaming app). Moreover, many infrastructure services regulated by the DSA have little relevance for DMA (e.g., WiFi operators, or VPN services). The DMA puts comparatively much more emphasis on infrastructure. For instance, virtual assistants and operating systems are not under the scope of the DSA. Advertising services can be regulated by the DSA but only some of them (e.g., storage and distribution of third-party advertisements).

Both the DSA and DMA did not specifically address the question of generative artificial intelligence services. However, both regulate AI as it is incorporated into regulated services, such as social media, or search engines. If they are embedded into regulated services, their regulation is always possible, especially under the DSA for VLOPs and VLOSEs. Even self-standing generative AI services, such as ChatGPT, might be regulated by the DSA and DMA as

[19] The coverage of browsers under the DSA can be contested, see Article 3(g)(i) ["a 'mere conduit' service, consisting of […] the provision of access to a communication network;"].

online search engines if they are connected to the web search.[20] Under both regulations, only very large providers of such services would be regulated, as the DSA only regulates very large search engines (VLOSEs), and the DMA only gatekeeper-sized search engines.

Regulatory nature of the DSA/DMA

The DMA and the DSA formulate their legal expectations through a set of due diligence obligations or prohibitions. Some rules are prescriptive and narrow, others are prescriptive but open-ended, and finally, some grant a lot of discretion to companies and regulators. However, in all cases, the rules are meant to be self-executing enough so that companies can incorporate them upfront into their digital services and compliance processes.

Big companies under the DSA/DMA are subject to designation by the European Commission. The DSA thresholds are purely quantitative. Once the company reaches 45 million monthly active users in the EU for the regulated portion of the service, it ought to be designated by the Commission. Under the DMA, the threshold is a mixture of quantitative and qualitative thresholds, where the former creation presumptions that can be rebutted by companies.[21] This process is subject to judicial review by the General Court, and then the European Court of Justice. The first months of the law clearly show that companies are actively using judicial review under the DSA/DMA to clarify legal concepts.

Under the DMA, the key issues related to the delineation of the scope of CPS services (*Apple v Commission,* T-1080/23, *Meta v Commission*, T-1078/23), but also the process of rebutting the presumption (*TikTok v Commission*, C-627/24 P). Finally, one case concerns the non-designation decision of the Edge browser by a competitor (*Opera Norway*, T-357/24). Under the DSA, the key issues related to the scope of regulated services (*Zalando v Commission*, T-348/23), and user counting (*Zalando v Commission*, T-348/23; *Amazon v Commission,* T-367/23; *Technius v Commission,* T-134/24; *Webgroup* v Commission, T-139/24; *Aylo v Commission*, T-138/24). There is no dispute against

[20] This because the definition of online search engines Article 3(j): "an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found." Since almost identical definition is applicable under the DMA (see Article 2(6) DMA, and Article 2(5) Regulation (EU) 2019/1150 (Platform to Business Regulation)); for additional discussion, see Botero Arcila, Beatriz, Is it a Platform? Is it a Search Engine? It's Chat GPT! The European Liability Regime for Large Language Models (August 12, 2023). Journal of Free Speech Law, Vol. 3, Issue 2, 2023, Available at SSRN: https://ssrn.com/abstract=4539452. Based on public disclosures, ChatGPT is inching toward the VLOSE status, see https://help.openai.com/en/articles/8959649-eu-digital-services-act-dsa

[21] See more detail in the institutional FIDE report: Paul-John Loewenthal, Cristina Sjödin and Folkert Wilman, Europe's Digital Revolution: The DSA, the DMA, and Complementary Regimes (2025).

non-designation under the DSA, even though there are some services whose non-designation status might be disputed (e.g., Spotify, Telegram, advertising platforms). However, under the DSA, it is harder to seek redress against non-designation because the Commission does not make such decisions formally.[22]

The institutional report says that the designation process seems to "work rather well."[23] I do not disagree, but I also see several important points for improvement. The DSA might benefit from a notification mechanism that exists under the DMA. The Commission should make decisions about non-designation too, so it is easier for third parties to contest such decisions as is the case under the DMA. Moreover, both laws might benefit from an administrative process that would allow third parties to initiate a process of designation, especially for companies that are unwilling to see themselves regulated. The Commission should also aim to clarify how it understands the scope of CPS services and DSA-regulated services. Under the DSA, DSCs might consider providing voluntary registries which would allow companies to gain more clarity about which rules apply to them and for which of their services.

Enforcement and supervision

Compliance with the DSA/DMA can be only achieved by combining persuasion (dialogue and guidance) and coercion (fines or orders). The first year of the DSA/DMA has been overall marked by more coercion, especially under the DSA. This might be explained by the need to mark a shift from non-regulation and gain respect for the regulatory framework.

However, overemphasis of coercion is not sustainable in the long run. Neither is it the most appropriate main strategy of compliance given that the Commission encounters the same companies over the years in repeated interactions. That is not to say that coercion should not be used, however, it must be used strategically in the areas where companies are unwilling to move their positions without it. Coercion via fines and orders is a costly process for business but also for the regulator. Every investigation ties a lot of resources into the process of collecting evidence, deciding, explaining the decision, and eventually defending it before the CJEU. If coercion is coupled with enforcement of open-ended provisions, or those that give a lot of discretion to companies, prevailing is even more costly for the regulator. Enforcement of open-ended provisions often requires evidence, and investigation of industry practices to establish due diligence benchmarks. Under the DSA, the Commission currently has 9 pending investigations,[24] all with a rather broad scope. Concluding all of them

[22] According to the case law, if such an applicant could seek direct annulment of an act according to Article 263, it can also pursue an action against a failure to issue an act. See Husovec, *Principles of the Digital Services Act* (n 6) 181.

[23] See Loewenthal, Sjödin and Wilman (n 21) 38.

[24] See ibidem, footnote 209.

means spending a lot of resources that cannot be used for dialogue and guidance that can have a more immediate impact on users.

At the time of writing, the Commission has only produced one piece of guidance on elections,[25] although two others, on trusted flaggers and protection of minors, are on the way. Some of the commonly occurring problems, such as data access for researchers (Article 40(12)) and notification of illegal content (Article 16), which the Commission is investigating were not subject to previous guidance or dialogue by the Commission. This means that investigations were started before the companies could have been potentially more easily persuaded to change their positions without locking resources into an expensive multi-year legal fight. This is sometimes unfortunate because once an investigation begins, companies are also internally limited in their ability to change their positions, so the investigation can slow down rather than speed up compliance. This problem is less visible under the DMA where only 6 more narrow investigations are being undertaken.[26]

However, regulatory theory and practice in some other areas suggest that enforcement actions are only part of the clout of the regulator,[27] and although they are helpful in achieving compliance, they must be used strategically. No one naively expects that companies will give up fights on some of the issues that are core to their business if the law provides some latitude for this, however, on many issues compliance can be achieved much more cheaply by persuasion.

This will free resources for the strategic use of coercion.

To be sure, it remains very important the Commission acts swiftly and decisively whenever it sees clear and simple violations that are not remedied voluntarily. This is how it builds its reputation and will undoubtedly incentivise companies to better comply with the DSA. Such swift and decisive actions can achieve long-term cooperation from companies. However, due to resource constraints, it will never be possible to achieve perfect compliance only through coercion.

Thus, one of the challenges for the European Commission in the coming years will be to develop a culture of dialogue and persuasion, next to its enforcement actions. This is a novel role for the Commission, especially given that many of its rules, processes and experts come to the DSA/DMA enforcement from competition law that works as an ex-post regime. And it might be also

[25] European Commission, 'Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections' (26 March 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707

[26] See Loewenthal, Sjödin and Wilman (n 21) 70.

[27] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) 21; John T Scholz, 'Cooperative Regulatory Enforcement and the Politics of Administrative Effectiveness' (1991) 85 American Political Science Review 115; see Husovec, *Principles of the Digital Services Act* (n 6) 456 ff.

counter-intuitive given that the Commission has gained unprecedented powers to enforce regulations centrally and exclusively.

Unlike the DSA, the DMA has an explicit procedure for regulatory dialogue. The so-called specification procedure (Article 8(2) DMA) has a regulatory rather than a sanctioning function. As noted by the institutional report,

> [...] the key feature of the DMA's specification process, which also sets it apart from the non-compliance proceedings, is its regulatory as opposed to sanctioning function. The purpose of specification is indeed to determine in a more granular manner what a particular gatekeeper should do to comply with a specific obligation, taking into account the specific circumstances of the gatekeeper and of its CPS. The guiding principles in this respect are the effectiveness in achieving the objectives of the DMA and of the particular obligation, and proportionality.[28]

The Commission currently has two pending specification procedures against Apple's iOS and iPadOS pursuant to Article 6(7). As noted by the institutional report, the benefits of such a procedure are that it can establish regulatory expectations in detail and faster. Moreover, the lack of sanctions for non-compliance with the specification decision might reduce some worries of regulatees that the decision itself can serve as a basis for follow-on litigation. The DSA lacks a similar process that would be often similarly helpful, especially for provisions like Articles 14(4), 28 and 35.

For the above reasons, it is important that the Commission embraces more dialogue and guidance in the coming years. It might take some inspiration from the work of Ofcom, although one could argue that the UK's regime has the opposite problem – too much guidance. The DSA intentionally imposed the cost of uncertainty on companies. However, that is not a reason to avoid reducing it if it delivers quick benefits to users. While dialogue is unlikely to push compliance on most commercially sensitive issues where companies are likely to fight, it can achieve a lot and save resources for the inevitable legal fights.

Critiques of the DSA/DMA

Even the biggest critics of the EU tech regulation seem to like the features that benefit them, such as regulation of their competitors, or limits on arbitrary moderation of accounts.[29] The two main criticisms of the DSA/DMA are that they kill innovation, and the DSA amounts to censorship.

The innovation objection against the DMA argues that the regulation will discourage new entrants by reducing incentives or making market entry overly

[28] See Loewenthal, Sjödin and Wilman (n 21) 66.

[29] Joe Rogan 'Joe Rogan Experience #2255 - Mark Zuckerberg' (*Youtube* 10 January 2025), https://www.youtube.com/watch?v=7k1ehaE0bdU (Zuckerberg criticising DMA but positively speaking of regulation of Apple); BBC, 'Meta to pay $25m to settle Trump lawsuit over ban' (30 January 2025), https://www.bbc.com/news/articles/c79d74nppvpo

expensive. Europe, in this argument, is shooting itself in the foot, and becoming less competitive. This narrative is very simplistic.[30] The innovation environment of any country has many other components that determine the success of businesses. Some forms of regulation encourage the entry of new businesses. Regulation can thus enable new businesses and innovations as much as it can prevent them.[31] The story behind the first generation of internet rules is a case in point.

More fundamentally, the criticism often assumes that innovation has some inherent "pure" trajectory which is only manifested under the conditions of unrestrained market forces. This obviously ignores that even in less regulation-prone countries, the governments always tilt the trajectory of innovation through many of their policies, ranging from intellectual property, and tax treatments to immigration policies. As eloquently put by Mazzucato, "[i]f the rest of the world wants to emulate the US model, they should do as the United States actually did, not as they say they did."[32] In other words, the US system itself has benefited tremendously from government interventions in the innovation ecosystem. Finally, it seems obvious, but worth highlighting anyway – not all innovation is a net benefit for society or has desirable re-distributive effects.[33]

Thus, the debate between regulation and innovation is hardly useful in the abstract, as one needs to know what specific rules are being discussed to be able to assess their impact on innovation and others.

The period from the E-Commerce Directive until the DSA/DMA, that is 2000–2020, was relatively quiet on the front of industry-specific rules for digital services. The EU even adopted a specific IP right for databases to incentivise investments into advanced data processing systems.[34] Yet, as noted also by the institutional report, the EU businesses mostly lagged behind the most successful digital services. This clearly shows that the reasons for this are not really caused by the presence or absence of industry-specific regulation. If anything, as I stated earlier, the EU rules enabled the EU-wide digital ecosystem by rejecting stricter forms of liability across the region. Thus, the sources of problems of European competitiveness and innovation ecosystems are much larger.[35]

---

[30] See Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 118 Nw U L Rev 2; Pierre Larouche and Alexandre de Streel, 'The European Digital Markets Act: A Revolution Grounded on Traditions' (2021) 12(7) Journal of European Competition Law & Practice 542.

[31] See examples provided by Larouche and de Streel (n 30) 544 (e.g., postal, telecommunication, finance).

[32] Mariana Mazzucato, *The Entrepreneurial State* (Anthem Press 2013), 1.

[33] See generally, Daron Acemoglu and Simon Johnson, *Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity* (PublicAffairs 2023).

[34] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20.

[35] See Mario Draghi, 'The Draghi Report' (*European Commission* 9 September 2024), https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

The DSA and the DMA have the potential to significantly reshape the power relationships between EU users and tech companies. However, their contribution to the actual contestability of the underlying digital markets 'owned' by gatekeepers is probably going to be more modest exactly because it mostly recalibrates their appropriability in favour of complementary incremental innovation.[36] To achieve a see change, the European innovation ecosystem requires a boost via a broader set of innovation policies to which the DSA/DMA are likely only a complement.

The second criticism levelled by the second Trump administration concerns allegedly censorial features of the DSA. The public comments by JD Vance or Elon Musk show a great deal of misunderstanding of what the law does, or what the powers of the Commission are. JD Vance presented the view that the EU Commission can annul elections or block websites for DSA violations, and Elon Musk that he was offered secret deals[37] — neither of which is true. The Chair of the Federal Communications Commission called the DSA's approach "something that is incompatible with both our free speech tradition in America and the commitments that these technology companies have made to a diversity of opinions," and Zuckerberg labelled it "institutionalised censorship."[38]

The DSA has two main components: content moderation rules, and risk management rules. Both types of rules are complemented by transparency. The content moderation rules force companies to better explain their decisions, and handle appeals so that individuals know why their content is blocked, demonetised, or accounts suspended. Risk management rules ask companies to redesign their services in favour of transparency, and sometimes more user empowerment (e.g., to be able to opt out from default recommender systems). For both types of rules, compliance can be localised.
Presumably, when the US administration talks about the censorial effects of the DSA, they refer to the removal of hate speech and the general risk management system that requires US social media to assess the risks on their services, audit them, and then improve, including with respect to their impact on electoral processes. I will address these concerns below in the DSA section in more detail. At this point, I want to make three observations.

---

[36] See for a fuller discussion, Larouche and de Streel (n 30) 548 ff; Pablo Ibáñez Colomo P, *The New EU Competition Law* (Bloomsbury 2023) 133 ff.

[37] See Euro News, 'Elon Musk claims EU offered an ‚illegal secret deal' as X charged with DSA breaches' (12 July 2024), https://www.euronews.com/next/2024/07/12/elon-musk-claims-eu-offered-an-illegal-secret-deal-as-x-charged-with-dsa-breaches; In February, Vice President JD Vance denounced content moderation at an AI summit in Paris, calling it "authoritarian censorship."; Foreign Policy, 'The Speech That Stunned Europe' (18 February 2025), https://foreignpolicy.com/2025/02/18/vance-speech-munich-full-text-read-transcript-europe/; x

[38] Reuters (n 10). Politico, 'Zuckerberg's censorship claims were 'misleading' — EU tech chief' (January 2025), https://www.politico.eu/article/mark-zuckerberg-meta-misleading-censorship-henna-virkkunen/

- Firstly, European legislatures have for a long time maintained different decisions about what speech must be prohibited. Such democratically adopted rules are not censorship only because they do not align with the case law of the US Supreme Court. Europe has its own tradition of freedom of expression. European Convention on Human Rights expects the European countries to outlaw expressions that cannot be outlawed in the United States, such as many forms of hate speech. In contrast, on matters of national security, the US case law can be seen as too willing to sacrifice freedom of expression from the EU perspective.[39]
- Secondly, as I explained, the DSA does not allow the European Commission to create new content rules, and thus it cannot 'censor' anything lawful. If it expects companies to remove unlawful content, it is because some legislature in the EU made a democratic decision that such content should be illegal in some circumstances.
- Thirdly, nothing in the DSA expects companies to comply with such rules on illegality outside of the European Union. Companies are thus permitted to localise the compliance. Arguably, the *de facto* Brussels effect of the DSA is going to be weak.[40]

Consumer awareness

To assess the success of the DSA/DMA, it is not only important to evaluate the experiences of regulatees and experts.

The perceptions of consumers and citizens are as important. To ensure that consumers understand what is at stake, it is important that legislators, policymakers and consumer organisations proactively inform consumers about the intended impact of legislation. This may require campaigns to make consumers aware of their rights[41] and to explain that inconvenient short-term effects pursue a higher and more long-term goal. There is a risk that companies will use various tactics to misrepresent the effects of the laws, or sometimes blame everything on the regulation.

However, the campaigns need to be candid about the trade-offs involved. Risk assessment for each new feature that can have a critical impact on consumers

[39] *TikTok, Inc. v. Garland*, 604 U.S. (2025). While the decision has similar logic to the EU Schrems cases (see n (18)), it goes much further because the US law was clearly equally adopted to counter the concerns about Chinese propaganda. ECtHR currently hears a comparable case against Ukraine (*Artur Volodymyrovych BOYAROV against Ukraine* App no 79083/17 (ECtHr, 16 September 2024); European Information Institute, 'Third-Party Intervention by European Information Society Institute (EISi) in re Artur Volodymyrovych BOYAROV against Ukraine Application no. 79083/17 (5 November 2024), available at https://husovec.eu/wp-content/uploads/2025/01/Boyarov-v.-Ukraine-Final-Public.pdf).

[40] Martin Husovec and Jennifer Urban, 'Will the DSA Have the Brussels Effect?' (*Verfassungsblog*, 21 February 2024).

[41] For instance, to consent to the combination of their personal data under Article 5(2) DMA and to port their data free of charge under Article 6(9) DMA.

(Article 34) might mean that European consumers will not be the first market for the roll-out. Some features might not be available in Europe because companies decide not to offer them for regulatory concerns. Other times, the convenience might be traded against fairness.

For example, as a result of the DMA, Google Maps is no longer prominently displayed at the top of Google's general search results when you search for a location. As a result, users will no longer immediately find a link in Google's general search results to open the relevant map for the location they are searching for, but will have to go to the Google Maps website to find the relevant map. The average user will probably find this inconvenient, as it takes a little more time and effort to access the map than the experience we are used to. However, these changes are aimed at making markets more contestable and fairer by giving other businesses a chance to attract consumers.

Trade-offs like these must be explained to consumers to increase their understanding of why these laws exist. Otherwise, companies might misrepresent the law to claim that any discomfort, overreach or deterioration of their online user experience is "the fault of the EU." Other industries, such as the food industry, face a lot of inconvenience too, but people already understand that access to the cheapest low-quality products is not always in their interest.

Private enforcement

Scholars seem to broadly agree that the DSA and DMA are capable of being enforced privately before national courts in parallel to public enforcement.[42] This includes strong possibilities of collective redress under EU consumer law (Article 42 DMA; Article 90 DSA), and possibly national extensions under unfair competition laws, or tort law. National experts seem to have a positive view of the prospects of such litigation. However, in the DMA context, there are concerns about potential retaliation by the gatekeepers against business users.

Under both acts, the Commission benefits from a protective mechanism for its adopted decisions (Article 39(5) DMA, Article 82(3) DSA). The provision

[42] Husovec, *Principles of the Digital Services Act* (n 6); Folkert Wilman, Saulius Lukas Kalėda, and Paul-John Loewenthal, *The EU Digital Services Act* (OUP 2024) § 54; Benjamin Raue and Franz Hofmann, *Digital Services Act: Article-by-Article Commentary* (Bloomsbury Publishing 2024) § 54; See Lena Hornkohl and Alba Ribera Martínez, 'Collective Actions and the Digital Markets Act: A Bird Without Wings' (2023) The Antitrust Bulletin; Josef Drexl, Beatriz Conde Gallego, Begoña González Otero, Liza Herrmann, Jörg Hoffmann, Germán Oscar Johannsen, Lukas Kestler & Giulio Matarazzi, Position Statement of the Max Planck Institute for Innovation and Competition of 2 May 2023 on the Implementation of the Digital Markets Act (DMA), 72 GRUR International 875 (2023); Rupprecht Podszun, 'Private Enforcement and Gatekeeper Regulation: Strengthening the Rights of Private Parties in the Digital Markets Act,' 13 JECLAP (2022), 254; Björn Christian Becker, 'Privatrechtliche Durchsetzung des Digital Markets Act' ZEuP 403 (2023); Assimakis Komninos, 'Private Enforcement of the DMA Rules before the National Courts' (*SSRN* 5 April 2024), https://ssrn.com/abstract=4791499

is inspired by Article 16(1) Regulation 1/2003 that applies in EU competition law.[43] The mechanism does not stop national courts from being able to seek different views from the Court of Justice of the European Union.

Another type of private enforcement is when technology companies start using the EU law as a protective shield against pre-empted national rules. This is especially likely under the DSA which has a broad scope combined with the effects of full harmonization. As a result, the regulation can help companies to set aside national rules that conflict with common EU rules, and seek invalidation of any decisions that are adopted on their basis. In the context of the DSA, we see the first such cases, and are likely to see more. This type of private enforcement actually does the Commission's job as the guardian of the EU treaties by protecting the internal market from becoming unjustifiably fragmented.

Conclusions and recommendations

The empowerment of Europeans stands at the centre of DSA/DMA compliance. In these regulations, European governments demand concessions from other powerful non-state actors for their own people.

As noted by Draghi, Europeans need economic heft to be able to enforce their values.[44] Adopting new laws is not enough. In that sense, the DSA/DMA are only powerful in combination with the size of vibrant consumer markets that are too attractive an opportunity to avoid for companies.

In the increasingly aggressive global environment, preserving and expanding the user empowerment protected by the DSA/DMA is becoming ever more vital. As shown by the second Trump administration, foreign companies can conspire with their governments to push back against European plans to empower their citizens. To preserve it, Europeans must have a good position to push back. But Europeans must also be able to defend as sensible everything that these laws do.

As explained above, my general recommendations for the DSA/DMA are as follows:

- The supervision and enforcement of the DSA and the DMA should be insulated from external and internal politics and allocated to an independent agency;
- The designation process under both the DSA and DMA should allow for third parties to initiate the designation process and should be followed by a formal decision even if it is negative, to facilitate judicial review;
- The Commission should prioritise persuasion (dialogue and guidance) and combine it with the strategic use of coercion (fines and orders) to speed up compliance for users and save resources for inevitable legal fights;

[43] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L 001.

[44] Draghi (n 34) 5.

- The Commission should issue guidance on how it understands the key concepts, such as core platform services, and online platforms;
- Stakeholders and regulators should increase consumer awareness about the new types of user empowerment and their rationale.

Section 2: Digital Services Act

Goals and Background

The Digital Services Act has three components.

First, the DSA is a tool for users to better understand how and why companies make decisions about their online activities. Second, the DSA is a regulatory system that forces companies to change the design and processes to better protect their users. Finally, it is a tool for society at large, including victims, NGOs, and law enforcement, to enforce the existing rules about what is illegal to do or say also in the online environment.

The DSA itself is a regulation,[45] accompanied by an implementing regulation[46] and delegated acts that can be adopted by the European Commission. To this date, the Commission has adopted delegated acts on supervisory fees,[47] audits,[48] transparency reports.[49] Delegated acts on counting of users and access to data by vetted researchers will be adopted soon.[50]

---

[45] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), O.J. (L 277) 1 EU.

[46] Commission Implementing Regulation (EU) 2023/1201 of 21 June 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council ('Digital Services Act') [2023] OJ L159/21.

[47] Commission Delegated Regulation (EU) 2023/1127 of 10 May 2023 supplementing Regulation (EU) 2021/784 of the European Parliament and of the Council by laying down rules on the procedures for issuing, reviewing, and lifting orders to providers of hosting services regarding terrorist content online [2023] OJ L149/23.

[48] Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines [2023].

[49] Commission Implementing Regulation (EU) 2024/2835 of 4 November 2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council [2024].

[50] European Commission, 'Questions and Answers on identification and counting of active recipients of the service under the Digital Services Act' (31 January 2023), https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers; [Draft] Commission delegated regulation (EU) .../... of XXX supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data pursuant to Article 40 of Regulation (EU) 2022/2065 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act

The DSA sets out its scope around the terms of safety, trust and predictability. This means that the law is claiming a lot of ground as its own. This fact is confirmed by numerous provisions that are drafted broadly. The definition of illegal content extends to anything that is unlawful to say or do in at least one of the Member States.[51] The risk management system also extends to all risks posed by illegal content, and any fundamental right.[52] Content moderation provisions procedurally cover decisions made by platforms based on illegality and contractual breaches ("ToS violations").[53] Thus, the DSA is a horizontal law that deals with almost everything that platforms do for and against their users.

As I have argued elsewhere,[54] we should measure the success of the law by how well it empowers the EU citizens. If Europeans improve their understanding of how decisions are made about them, feel more protected against unlawful activities of others, and are more able to seek correction of mistakes, the DSA will be successful.

But safety cannot be simplified as top-down state-imposed minimisation of all possible risks. Individuals need risks to become more resilient through learning. This is why I tend to emphasize that trust is equally important in the future enforcement of the law. Most of the time, safety promotes trust. But sometimes, it is at odds with it. In those cases, it needs to be balanced with the agency of individuals and their ability to make their own choices.[55]

Unlike many other laws, the DSA creates legal mechanisms that presuppose an existing ecosystem of other non-state players. The goal is to avoid concentrating all the power with either platforms, or the state. These non-state players include professional notifiers of illegal content who help victims or defend the public interest, users' groups that represent content creators, out-of-court dispute settlement bodies who provide external appeals services, researchers who study the risks and mitigation strategies, etc. As I argued after the adoption of the DSA in November 2022,

> My main concern about the DSA resides also in its strength – it relies on societal structures that the law can only foresee and incentivize but cannot build; only people can. These structures, such as local organisations analysing threats, consumer groups helping content creators, and communities of researchers, are the only ones to give life to the DSA's tools. They need to be built bottom-up and sometimes locally in each Member State. If their creation fails, the regulatory promises might turn out to be a glorious aspiration.[56]

---

[51] Digital Services Act, art. 3(h).

[52] Ibidem, art. 34.

[53] Ibidem, art. 17, 20, and 21.

[54] Husovec, Rising Above Liability: *The Digital Services Act as a Blueprint For the Second Generation of Global Internet Rules* (n 4); Martin Husovec, 'Will the DSA work' in Joris van Hoboken et al. (eds), *Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsbooks 2023).

[55] Husovec, *Principles of the Digital Services Act* (n 6) 465.

[56] Husovec, 'Will the DSA work' (n 54) 21.

The DSA only offers incentives for these social structures. In the first official evaluation of the law, the Commission should empirically interrogate if these incentives are always strong enough, and, possibly, if they are not too strong in some cases.

From this perspective, the first phase of the DSA rollout must focus on institutions. In February 2025, we still do not have a fully functioning institutional set-up. While the Commission machine is up and running, five Member States still have not fully institutionally prepared their national regulators, or even designated them.[57] This means they cannot shape the European system, and supervise companies that are in their orbit, that is, established in their jurisdiction. For instance, before Belgium adopted its law, Telegram, which has a Belgian legal representative, could not have been supervised by anyone, as the Commission's powers only start with the designation as a VLOP.

In terms of non-state actors, the data access for researchers is still not fully in place because the Commission has not yet formally adopted the Delegated Act for vetted researchers. This should happen soon. The certification of trusted flaggers and out-of-court dispute settlement bodies is in full swing, but some shortcomings are becoming clear. The Commission's website currently lists 20 certified trusted flaggers,[58] especially with a focus on the protection of minors, consumers and intellectual property rights, but many countries remain without a trusted flagger. It seems like the promises made by the DSA to trusted flaggers in Article 22 are not always sufficient to attract enough players to seek certification for their activities in exchange for a decision fast-lane and technological privileges. There is a general sense that the trusted flaggers often lack the resources to do their work.

The out-of-court dispute settlement bodies are slowly coming to existence too and have already received thousands of cases.[59] There are six such bodies to this date,[60] and several other applicants in the pipeline. The certified ODS bodies were granted certification in Austria, Germany, Hungary, Malta, Italy and Ireland. They cover English, German, Italian, Dutch, Spanish, Maltese, Hungarian, French, and Portuguese.[61] Most of the ODS bodies focus on major social media companies. Thus, many speakers of smaller languages yet lack

[57] Poland, Czech Republic, Spain, Portugal, and Cyprus. See https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081

[58] European Commission, 'Trusted flaggers under the Digital Services Act (DSA),' https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

[59] Daniel Holznagel, 'Art. 21 DSA Has Come to Life' (*Verfassungsblog* 5 November 2024), https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification/; Appeals Centre Europe, *Transparency Reports*, https://www.appealscentre.eu/transparency-reports/; Appeals Centre Europe, 'Users Make Voices Heard as Appeals Centre's First Decisions Overturn Platforms' (10 March 2025).

[60] European Commission, 'Out-of-court dispute settlement bodies under the Digital Services Act (DSA),' https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement

[61] One ODS body covers all languages, but offers services only in English, German, French, Italian and Dutch.

the option of an external appeal in practice. Moreover, even among these languages, some subject matters might not have respective ODS bodies.

While the NGOs are starting to engage in private enforcement of the DSA,[62] it does not seem that mainstream collective interest groups, such as trade unions or trade associations, have already internalised the possibility of helping their constituencies with content disputes as professional user groups.[63] There is thus a long way to go on the awareness among those who are empowered by the law. In other words, the ecosystem of players that the DSA envisages is still not fully in force.

The DSA's scope

The DSA relies on terms developed under the first generation of rules, where the terms determine only whether a particular provider benefits from liability exemptions. The DSA divorced these terms from their origin and introduced them into Chapter 1 as concepts that open the scope of the DSA in general. As a result, the potential application of Chapter 2 (liability exemptions) and Chapter 3 (due diligence obligations) are independent of each other. While this is clear from the legislative history, in *Zalando v Commission*,[64] an online marketplace attempts to infuse the meaning of the pre-existing case law on liability exemptions into the terms themselves, and thus undercut the applicability of Chapter 3. The General Court is expected to clarify this issue soon.

Due diligence obligations and liability exemptions play different roles, even though they are both given to the services that are defined through the same terms. The analogy one can use to explain this is that of banks and money laundering. Banks can become co-conspirators and be liable for individual attempts to launder money. However, in most cases, they are not co-conspiring in such ways. Thus, to motivate them further, the law imposes due diligence obligations in the form of anti-money laundering rules that are meant to minimise such occurrences or make it more difficult. Violating such due diligence obligations triggers fines and supervision but does not make one a criminal or money launderer.

The DSA is very similar. Chapter 2 draws the line between co-conspirators who potentially act in concert with their users and those who do not, while Chapter 3 imposes general expectations of due diligence on the industry. Even as a co-conspirator, that is, someone losing liability exemptions, one can violate due diligence duties, but it is not going to be the worst thing that can happen to such a person, as other laws, for example, criminal law, have free reign at that point too (c.f., the French case of Mr Durov, the CEO of Telegram).[65]

---

[62] LG Berlin, judgement of February 6, 2025 – 41 O 140/25 eV.

[63] Digital Services Act, art. 86.

[64] Case T-348/23 [2023].

[65] BBC, 'Telegram founder allowed to leave France following arrest' (17 March 2025), https://www.bbc.co.uk/news/articles/cg703lz02l0o

The terms used by the DSA – mere conduit, caching, hosting, online platforms, search engines – are all sufficiently broad to be future-proof. They describe technical functioning and not products, or business models.[66] The basic technical reality is unlikely to change. That is, digital services will continue to store other people's information at their request and distribute it to the public.

That being said, it is not always possible to separate the storage of non-editorial content of users from editorial content. While the DSA does not have explicit provisions to this effect, as indicated by the definition of "online platforms,"[67] if users cannot separate the two types of content in their user experience, the service remains regulated. For this reason, the DSA inevitably, at least for purposes of some provisions, such as protection of minors, or risk management, also regulates digital services that mix the two together (e.g., Google Maps). This serves as an incentive for companies to decouple the two types of content if possible or comply with the obligations for user-generated content *and* other inseparable features.

Aside from the hybrid services, the scope issues have also arisen also in other contexts. The qualification of live-streaming remains difficult, albeit somewhat mitigated by the fact that live-streaming is rarely only a stand-alone service and is usually integrated into broader regulated services, such as social media. The interpretation of the economic character of services that is important to open the scope of the DSA will at some point have to be clarified by the CJEU. At the moment, the General Court has an opportunity to do so in *Apple v Commission*.[68]

Finally, there are potentially some unforeseen effects in using the terms from the liability exemptions in the new context. This has become a problem for some services that have several providers within the same digital service, for example, social media as an overarching hosting service, that has owners of groups that can be said to host material of their users. Such layered structure is typical for the internet as most blogs have their own hosting providers, and they might have their own hosting providers.

For liability exemptions, this did not cause any problems, as it only multiplied the number of beneficiaries of the liability exemptions. However, within the due diligence system for individual digital services, this causes difficulties, especially if applied to the smallest communities on those services. If the DSA is understood as a regulatory tax on central decision-making of providers of digital services, then the smallest community components of the ecosystem within such services should not be regulated as providers in their own right. This is intentionally why community-based content moderation is outside of the scope of the DSA's procedural duties.

[66] Digital Services Act, Recital 29.
[67] Ibidem, art.3(i); Husovec, *Principles of the Digital Services Act* (n 6) 167 ff.
[68] Case T-1080/23 [2023].

Thus, for instance, an owner of a group on a social media site should not be considered hosting for due diligence purposes, while it should be for liability exemption purposes. Currently, there is no explicit consideration of this problem in the DSA itself. If a term is applicable per Chapter 1, it triggers both Chapters 2 and 3 equally. In the future, the legislature might want to consider clarification on the scope of hosting services in particular, as their obligations are not qualified by size. It might be counterproductive to expect that small communities comply with Articles 17 and 18, even though they should benefit from the liability exemptions. One possibility would be to offer an explicit carve-out from hosting and online platform tiers of obligations for such entities.

Due diligence obligations

The DSA due diligence obligations cover three main areas: (a) content moderation process, (b) risk management on services, and (c) transparency.

Content moderation obligations (Articles 14, 16, 17, 18, 20, 21) are meant to improve the decision-making process by subjecting decisions to prior disclosure of rules, explanation of individual decisions, and provision of contestation mechanisms in form of internal and external appeals. Taken together, these provisions aim to reduce opacity and arbitrariness of the decision-making and increase predictability and fairness of the outcomes.

Risk management provisions relate online platforms, and they either take form of prescriptive design obligations (Articles 25, 26, 27, 28) or general risk management system for VLOPs/VLOSEs (Articles 34-35). In essence, all online platforms operated by mid-sized companies must protect minors and consumers, however, only VLOPs/VLOSEs must conduct ongoing risk assessments and audits also for other types of risks.

Transparency obligations underpin both content moderation and risk management rules. The DSA forces mid-sized regulated companies to publish bi-annual content moderation reports (Article 15), submit their statements of reasons to a centralised database (Article 24), and give access to researchers and publish risk assessments, audits and implementation reports if they are VLOPs/VLOSEs (Articles 40, 42).

It is too early to say how these due diligence obligations will influence the quality of the user experience on digital services. While some questions might turn on the exact interpretation of the rules, there are several provisions that require dialogue and coordination to establish useful compliance practices. One such example relates to enforcement of illegal content.

Content moderation

The DSA sometimes limits the scope of mechanisms to illegal content due to considerations of freedom of expression (e.g., Article 16, 22, 23, etc.). This is

often motivated by the fact that assessing illegality must be treated differently from pure contractual breaches of rules that are not mandatory for platforms. The problem is that companies prefer to decide everything against their own terms and conditions because this allows them to save resources compared to assessing conduct and behaviour against a multitude of national laws. Plus, platforms often act globally against ToS violations, and tend to localise compliance with illegality-based notifications, as not all countries must consider the same content illegal.

In other words, there are many efficiencies and other good reasons behind such an approach of companies. It is therefore no surprise that companies encourage their users to report content primarily as ToS violations, and not as illegal content. And it is possible that users find it more user friendly too.

The problem is, however, that if mechanisms for illegal content in the DSA are only applicable if the content is *notified* or *assessed* against a specific national law, as opposed to when it actually *is* against a specific law, the companies effectively would not be implementing some of the DSA provisions (e.g., suspension of accounts of repeated offenders), or publicly reporting numbers that are not very helpful (e.g., how much illegal content they took down).

Thus, what is needed is more cooperation. For instance, the companies and regulators could initiate a close upfront mapping of the terms and conditions violations against the illegality rules in the EU Member States. Such mapping would allow companies to continue deciding against their own terms and conditions, but would internalise that some of such decisions are in parallel also about illegal content (e.g., a breach of harassment policy is also the case of illegal behaviour in some cases). If the regulators were to insist that objective illegality is always what triggers the application of the various illegality-only provisions, the only way to comply with such interpretation would be to over-implement the DSA to apply to all scenarios. In contrast, if companies can read the rules based on the channel which the notifications arrive at their doors, many DSA provisions will never be activated.

Thus, it seems that the best way out of a difficult situation is to try to find middle-ground solutions, such as pre-mapping of terms and conditions against rules on illegality, and then allow companies to decide against their contractual rules, however, internalise consequences for the process and transparency as if these cases concerned illegality.

Out-of-court dispute settlement bodies

Another key area in terms of coordination is the out-of-court dispute settlement system. Article 21 of the DSA created conditions for certification of non-state bodies interested in the role. At the time of writing, five bodies were certified.

Three bodies are at no cost to complainants, and two charge symbolic fees (5–10 euros). That means that all the cost is borne by the online platforms (usually several hundred euros).

This is a result of the provisions that indicate that "for recipients of the service, the dispute settlement shall be available free of charge or at a nominal fee" (Article 21(5)). This seems to have been interpreted by many not only as fees that are below the overall cost but as zero or symbolic fees. Such fee structure is obviously preferrable for the ODS bodies (and users) that can attract more complainants with no fee or symbolic fee than with fees that approach 50% of the overall dispute costs.

As a result, the ODS system has become costlier for online platforms. That per se is not as problematic because as we can see so far, even though Article 21 applies to all online platforms, not just VLOPs, the ODS bodies effectively conduct it only for a subset or all VLOPs. In other words, the potentially high cost of compliance for mid-sized platforms is being mitigated by the scope of certification of the ODS bodies that are not interested in the market around smaller online platforms or demand of users.

However, the problem is that VLOPs that are subject to this system already and are already requested to pay several hundred euros per dispute, regardless of whether their decisions are confirmed or rejected by the ODS bodies. In other words, they pay even if their decisions were found to be correct.

The only way that regulators can address this problematic incentive structure is to expect ODS bodies to differentiate the fees based on the outcome, or the procedural stage. This is a direct outcome of the complainants taking no risks when filing disputes under this fee structure. Many certified ODS bodies are already doing this. They are charging platforms lower fees in cases of self-correction by platforms, vexation complaints, or rejections on the admissibility stage. But in the absence of real fees for complainants, these are the only levers that can be used and demanded by the regulators and they still might turn out to be insufficient.

To be sure, it is too early to evaluate the ODS system. The system is clearly in operation, and Europeans are filing disputes, and sometimes complaining to the DSCs when the ODS decisions are not implemented. There are many questions of cooperation between ODS bodies and platforms that would require standardisation.

It is recommended that the European Commission invests resources in facilitating such a standardisation process. Standardisation can lower the overall costs of the system but also encourage entry by new ODS bodies. And as noted earlier, there are significant gaps in coverage when it comes to some languages at the moment.

Based on my conversations with stakeholders, including a workshop at LSE,[69] I am of the view that the following issues will sooner or later require some form of harmonisation:

1. Dedicated contact points on each side for technical, financial and legal issues;
2. Case matching methods (e.g., unique identifiers);
3. List of key information related to content moderation decisions, including:
   a. communication of cases where legal obligations prevent sharing of case data, such as for child sexual abuse material (CSAM),
   b. communication of cases where data is very sensitive;
4. Data retention periods for content moderation;
5. Procedural rules for the entire process:
   a. including admissibility and vexatious complaints policies,
   b. policies about "the EU nexus" for admissibility,
   c. rules about "default judgments";
6. Educational interventions to increase the visibility of the ODS bodies;
7. Transparency on the issuance of decisions and their follow-up implementation.

Designation of VLOPs/VLOSEs

The Commission has designated 23 VLOPs and 2 VLOSEs.[70] Based on recent disclosures, two additional services, namely WhatsApp and Waze, will be designated soon.[71]

The designation process under the DSA starts with companies publishing their disclosures of monthly active users (Article 3(p)) on their own websites. Unfortunately, Article 24(3) does not include any notification process for those companies that exceed the threshold or are close to the threshold of 45 million monthly active recipients of the service in the EU. Moreover, because the European Commission does not have the competence to formally investigate companies before they are designated, this results in a somewhat suboptimal situation where the Commission must rely on the national DSCs across the EU to do its job.

In the original Commission's proposal, the Commission was under an obligation to publish a delegated act on methodology for how to count

[69] I held a workshop at LSE in November 2024. The event brought together many leading ODS bodies and big and small online platforms to discuss the need for harmonisation of certain issues, such as those noted above.

[70] European Commission, 'Supervision of the designated very large online platforms and search engines under DSA' https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-metaplatforms

[71] Reuters, 'WhatsApp faces EU tech rules after reaching very large platform status' (19 February 2025), https://www.reuters.com/technology/whatsapp-faces-eu-tech-rules-after-reaching-very-large-platform-status-2025-02-19/

users.[72] However, the co-legislators, the European Parliament and Council, insisted on the optionality of such a provision. To clarify the concept, therefore, the final text includes Recital 77 which provides additional guidance that should be used to interpret Article 3(p). To this date, the Commission has not adopted the delegated act on counting users, although one is being prepared.

In *Zalando v Commission*, Zalando argues that the absence of a more specific methodology violates legal certainty and leads to unequal treatment between companies.[73] To the best of my knowledge, in all designations to date, the Commission has relied upon companies' data and only rejected various criteria that companies have used to reduce the overall numbers. Only in the context of the fee calculation, the Commission has used its own methodology. Thus, companies have a lot of discretion to overcome lack of certainty, and the Commission has a reduced ability to object to different methodologies as long as they are plausible.

That being said, the problem of **unequal treatment** can arise. It arises less in the context of designated services. For them, even if they report numbers that are not comparable, this is without consequence because the only relevant fact is that they exceed the threshold. However, if competitors adopt methodologies that underestimate numbers, this could lead to a situation where one competitor is subject to a regime while the other is not (e.g., WhatsApp vs Telegram). An additional complication is that for such scenarios, the Commission does not have the competence to investigate, and has to rely on the DSCs who are competent. As a result, the responsibility to assure equal treatment lies with the competent DSC. However, DSC might have insufficient information about other competitor VLOPs in that area.

The anticipated delegated act could address this problem. But the EU legislature should oblige the Commission to issue negative designation decisions, and have stronger investigatory powers for the purposes of Article 24(2) even before the companies are designated. The powers envisaged in Article 24(3) are limited given Articles 56(2) and (3). The proposal would thus require changes in the competencies of the Commission. The direct benefit of such change would be that the Commission's decision to not designate could be reviewed before the General Court, similarly as is the case under the DMA.

[72] See Article 25(2) of European Commission, *Proposal for a regulation of the European parliament and of the council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0825

[73] See my disclosure on page 1. I represent EISi as an intervener before the General Court.

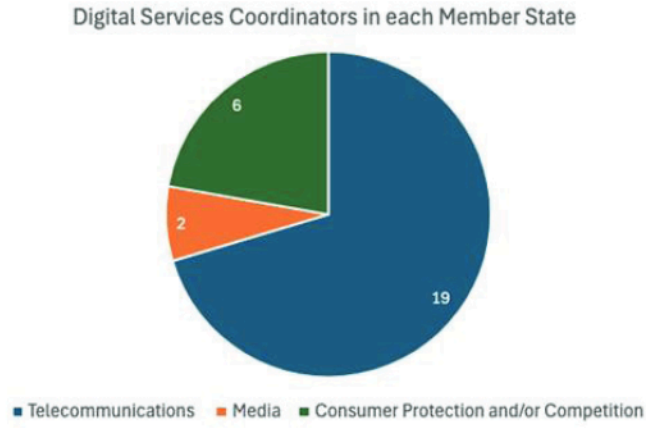
Figure 4. Details of VLOPs and VLOSEs

Type of service	Digital Service	COO	Company
Social media	Youtube	Ireland	Alphabet
	Facebook	Ireland	Meta
	Instagram	Ireland	Meta
	Tiktok	Ireland	Bytedance
	LinkedIn	Ireland	Microsoft
	Snapchat	Netherlands	Snap
	Pinterest	Ireland	Pinterest
	X/Twitter	Ireland	Twitter
App stores	Google App Store	Ireland	Alphabet
	Apple Store	Ireland	Apple
Marketplaces	Amazon Marketplace	Luxembourg	Amazon
	AliExpress	Netherlands	Alibaba
	Booking.com	Netherlands	Booking.com
	Temu	Ireland	Whaleco Technology
	Shein	Ireland	Infinite Styles
	Zalando	Germany	Zalando
Adult sites	Pornhub	Cyprus	Aylo Freesites
	Stripchat	Cyprus	Technius
	XVideos	Czechia	Webgroup Czech Republic
	XNXX	Czechia	NKL Associates
Price comparison	Google Shopping	Ireland	Alphabet
Maps	Google Maps	Ireland	Alphabet
Encyclopaedia	Wikipedia	Netherlands	Wikimedia
Search	Google	Ireland	Alphabet
	Bing	Ireland	Microsoft

Public enforcement

The public enforcement architecture around the DSA is unusual. Informed by the failures of the GDPR enforcement, the Commission was given partly exclusive and partly strong shared competence to supervise VLOPs and VLOSEs. All other companies are supervised exclusively by national regulators – Digital Services Coordinators (DSCs). Since there were no pre-existing national regulators in the area, the Member States had to either invent or pick an existing one. A great majority of the Member States designated telecommunications regulators, with a minority opting for media and consumer/markets regulators (see Figure 5). This variety is arguably a good thing as it brings more diversity of views which is much needed in an area as broad as regulation of digital services.

Figure 5. Types of Digital Services Coordinators



The overview in the comparison section details how Member States allocated resources to the DSA supervision and enforcement. As expected, the approaches differ significantly. On the one hand, Ireland has allocated significant resources, and on the other, some countries have only designated an authority but did not increase resources. A few countries have adopted special fees for online platforms; most others do not levy any fees on established platforms.

The DSA allows the Member States to allocate specific areas or provisions to other authorities. The overview below shows that several countries have done this, especially on provisions that relate to recommender systems, protection of minors, and consumer protection. The authorities competent for these provisions are often consumer or data protection authorities.

Figure 6. Non-DSC with DSA Competences

	Art 14	Art 18	Art 25	Art 26	Art 27	Art 28	Art 30	Art 31	Art 32	Art 37
Croatia										
Finland										
France										
Germany										
Greece										
Lithuania										
Slovenia										
Spain										
Sweden										

Legend: Blue: Data Protection; Orange: Consumer Protection; Green: Other.

Between 2023 and 2024, the only public enforcement has been taking place on the EU level. National regulators have not started their own investigations yet – although Irish DSC has requested a number of questions from regulatees on specific compliance issues.[74] To date, the Commission has launched a number of investigations against 6 services – AliExpress, Facebook, Instagram, TikTok, X, and Temu (see Figure 7). TikTok averted interim measures for a procedural violation of failing to submit ad hoc off-cycle risk assessment for a new feature of its service by accepting commitments.[75] Only the case against X/Twitter has progressed to preliminary findings.[76] Commitments were rejected by Elon Musk as "secret deal," which means that the case is likely to soon conclude with a non-compliance decision on a narrow set of issues.

- X/Twitter (December 2023),
- AliExpress (March 2024),
- Meta (April, May 2024),
- TikTok (April and December 2024),
- Temu (October 2024).

Thus, most of the investigations that were initiated by the Commission have not progressed to the stage of preliminary findings. The reason might be that as shown below, the scope of these investigations is often very broad, and includes even questions that would require a lot of fact-finding and additional evidence (e.g., Articles 28 and 35).

Figure 7. Pending DSA investigations

	Type of obligations	X = Twitter	TikTok	AliExpress	FB/Instagram	Temu
Standard obligations	Content moderation rules				14(1)	
	Content moderation process	16(5), (6)		16(1), (4), (5)	16(1), (5), (6)	
	Statement of reasons and appeals			20(1), (6)	17(1); 20(1), (3)	
	Dark patterns	25(1)			25(1)	
	Transparency				24(5)	
	Advertising			26(1)		
	Protection of minors		28(1)		28(1)	
	B2C marketplace obligations			30(1), (2), (7)		
	Recommender systems			27(1), (2)		27
Special obligations	Risk assessment	34(1), (2)	34(1), (2)	34(1), (2)	34(1), (2)	34
	Risk mitigation	35(1)	35(1)	35(1)	35(1)	35
	Recommender systems			38		38
	Advertising	39	39(1)	39		
	Transparency					
	Compliance function					
	Data access	40(12)	40(12)	40(12)	40(12)	40

[74] Coimisiún na Meán, 'Coimisiún na Meán opens review of online platforms' compliance with EU Digital Services Act' (12 September 2024). https://www.cnam.ie/coimisiun-na-mean-opens-review-of-online-platforms-compliance-with-eu-digital-services-act/

[75] European Commission, 'TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act' (5 August 2024). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161

[76] European Commission, 'Commission sends preliminary findings to X for breach of the Digital Services Act' (12 July 2024). https://digital-strategy.ec.europa.eu/en/news/commission-sends-preliminary-findings-x-breach-digital-services-act

In the meantime, the Commission has been busy defending its designation decisions before the General Court. There are currently six pending designation disputes (Amazon, Zalando, Xvideos, Stripchat, Pornhub, Xnxx),[77] none of which have been decided yet. The General Court, and Court of Justice of the European Union, however, already issued some procedural decisions. Their common starting point is that:

> [...] it must be emphasised that Regulation 2022/2065 is a central element of the policy developed by the EU legislature in the digital sector. In the context of that policy, that regulation pursues objectives of great importance, since it seeks, as is apparent from recital 155 thereof, to contribute to the proper functioning of the internal market and to ensure a safe, predictable and trusted online environment in which the fundamental rights enshrined in the Charter are duly protected.[78]
>
> In addition, the unprecedented speed – only 16 months – with which political agreement was reached on Regulation 2022/2065 demonstrates the urgency which the EU legislature has attached to the pursuit of that objective. That is particularly the case with regard to the enhanced due diligence obligations [..] which the EU legislature specifically decided to apply before the general entry into application of that regulation in the light of the systemic societal risks associated with those types of services [..].[79]

In *Amazon v Commission*,[80] Amazon sought an interim order seeking suspension of Articles 38 and 39 before the General Court decides on the merits of its invalidity pleas raised against the designation decisions. The President of the General Court initially granted it with respect to Article 39, however, on appeal, the European Court of Justice quashed the decision.[81] ECJ found that Amazon satisfied all the requirements for interim measures except for the balancing of interests. According to the Court, the effects of publishing ad archives are not existential for Amazon's business, and the downside can be somewhat restored, and/or ex-post compensated by money. Moreover, the public interest represented by the DSA is strong. Hence, Amazon has to comply with Article 39 while it awaits the ruling. The attempts of XVideos, YouPorn and Xnxx to seek the same interim measures equally failed.[82]

---

[77] Case T-367/23 *Amazon EU v Commission* [2023] ECLI:EU:T:2023:589, Case T-348/23 *Zalando v Commission* [2023]; Case T-138/24 *Aylo Freesites v Commission* [2024]; Case T-139/24 *WebGroup Czech Republic v Commission* [2024]; Case T-134/24 *Technius v Commission* [2024] (commonly referred to as *Stripchat*); Case T-486/24 *NKL Associates v Commission* [2024].

[78] Case C-639/23 P(R) *Amazon EU v Commission* [2023], para 155.

[79] This has been repeated by the General Court, see e.g., Case T-486/24 R *NKL Associates v Commission* [2024], para 111.

[80] Case T-367/23 *Amazon EU v Commission* [2023] ECLI:EU:T:2023:589.

[81] Case C-639/23 P(R) *Amazon EU v Commission* [2023].

[82] Case T-138/24 *Aylo Freesites v Commission* [2024]; Case T-139/24 R *WebGroup Czech Republic v Commission* [2024]; Case T-486/24 *NKL Associates v Commission* [2024]; Case Aylo Freesites LTD v European Commission Case C-511/24 P(R).

Moreover, in three out of six pending cases, the General Court had to decide about the ability of third parties to intervene to support either the European Commission or the plaintiffs. In *Amazon*, BEUC was allowed to intervene on the side of the Commission. In *Zalando*, the European Information Society Institute (EISi), after an appeal to the ECJ, has been allowed to intervene on the side of the Commission, while the German association of e-commerce, BEVH, was allowed to intervene on the side of Zalando. Finally, in *Stripchat* case, Article 19, a freedom of expression NGO, was allowed to intervene on the side of the Commission. In Stripchat and Zalando, the General Court has accepted that Article 86 of the DSA gives companies direct legal interest in these cases, which has made interventions easier than it is usually the case.[83] Thus, the Court has embraced the role of civil society in these cases.

Finally, the Commission has five pending cases concerning supervisory fees.[84]

Risk management and audits of VLOPs/VLOSEs

In November 2024, VLOPs/VLOSEs published the first batch of their systemic risk assessments and mitigations (SRAMs), audit reports, and audit implementation reports.[85] Although the public reports have been redacted, they unveil a great amount of detail about the risk management practices of technology companies. Even though the documents were primarily prepared for regulators, as opposed to the public, they will undoubtedly serve researchers, civil society, and other regulators who otherwise do not have access to such information. Civil society has been particularly critical of their lack of DSA-specific involvement in these audits.[86]

Risk assessment exercises entail considerable costs for all designated companies because they must prepare their SRAMs, prepare for audits, pay for audits, and spend time cooperating with auditors who try to validate SRAMs, which often means involving staff across the organisation for prolonged periods, and finally respond to findings of audit reports in a short period of time. Some industry players consider the pace of such annual audits too fast. Indeed, there is usually little time after the end of one cycle, to incorporate the learnings into the new cycle, which creates an odd situation for the following year. While the

---

[83] Krzysztof Pacula, 'Inquiry into the validity of the Digital Services Act and the role of the representative associations under that regulation' (2024) 25 ERA Forum 259.

[84] Case T-55/24 *Meta Platforms Ireland v Commission* [2024]; Case T-58/24 *Tiktok Technology v Commission* [2024]. Case T-66/25 *Meta Platforms and Meta Platforms Ireland v Commission* [2025]; Case T-88/25 *Tiktok Technology v Commission* [2025]; Case T-89/25 *Meta Platforms Ireland v Commission* [2025]; Case T-92/25 *Google Ireland v Commission* [2025].

[85] See an overview here: https://docs.google.com/spreadsheets/d/12hJWpCFmHJMQQlz1qkd6OgGsMW82YcsWgJHXD7BHVps/edit?gid=0#gid=0 (maintained by Alexander Hohlfeld).

[86] Center for Democracy & Technology, 'Civil Society Responds to DSA Risk Assessment Reports: An Initial Feedback Brief' (17 March 2025), https://cdt.org/insights/dsa-civil-society-coordination-group-publishes-an-initial-analysis-of-the-major-online-platforms-risks-analysis-reports/

overall costs of these exercises have not been officially disclosed by companies, they likely reach millions of euros per year per service.

The audits and audit implementation reports force companies to self-correct many non-compliance issues without the need for regulators to weigh in. Moreover, auditing often more closely looks at the types of non-compliance that would be hard to detect or monitor for regulators (e.g., governance, or whether a particular control was in place for the entire year, etc.). Published audits showed a great effort in decomposing the DSA obligations into the smallest auditable components.

The audits show that auditors tend to accept internal self-imposed benchmarks of companies or invoke procedural shortcuts when it comes to the questions of substantive interpretations of more complex provisions (e.g., Articles 14(4), 28, etc.). This is only a short-term problem. In the long run because as the authoritative interpretation of the DSA develops, the opacity of some of these provisions will be hopefully reduced. All this again suggests that the Commission can improve the specificity of such audits by adopting their own benchmarks as recommendations.

The auditing process itself has been criticised for being set up too late[87] and lacking more nuance in the evaluation system. Under the DSA, auditors must assign one of the following three marks: "positive," "positive with comments" or "negative" (Article 37(4)(g)). For instance, EY decomposed the DSA into 301 auditable obligations.[88] Based on the DSA's exact wording, if only one of them is not complied with, the audit outcome will be negative. That seems not only harsh but also misleading. The Commission might want to encourage complementary language by auditors, such as "overall positive," or "predominantly positive," or in percentages.

Furthermore, the Commission should explore whether the enhanced obligations for VLOPs/VLOSEs need to remain the same regardless of regulatees track record over the years. Currently, there are very different actors in the top tier, such as Meta and Alphabet on one hand, and Wikipedia, an NGO, or smaller companies on the other. Some of them are subject to many investigations or complaints, while others are subject to none. The key costs related to compliance with the enhanced obligations is annual auditing. To motivate companies, the DSA might borrow the mechanism of suspension from the DMA (see Article 9). The possible options could be to suspend the application of selected provisions in the VLOP/VLOSE tier or prolong the risk assessment cycle. VLOPs/VLOSEs anyway remain subject to an obligation to produce ad

[87] While the first designations took place in April 2023, the Delegated Act was adopted in October 2023, see European Commission, 'Delegated Regulation on independent audits under the Digital Services Act' (20 October 2023), https://digital-strategy.ec.europa.eu/en/library/delegated-regulation-independent-audits-under-digital-services-act

[88] Google Ireland Limited, *DSA Audit Implementation Report* (2024), https://storage.googleapis.com/transparencyreport/report-downloads/dsa-audit-google-implementation_2023-8-28_2024-5-31_en_v1.pdf

hoc off-cycle risk assessment whenever they introduce features that can have a critical impact on their risk profile (Article 34(1)).

Moreover, the VLOP designation under the DSA is becoming increasingly used in other acts of EU law, which does not always reflect their internal diversity.[89] It is often assumed that VLOP stands for Big Tech, which is hardly true. This is another aspect that should be carefully watched and analysed. Eventually, the EU legislature might consider if the status conferred in the broader EU legislation should not be subject to a qualitative threshold, along with the current quantitative threshold, that would test the impact of services on society at large. While the mechanism could be modelled after the DMA, the key problem would be properly defining the qualitative threshold that is subject to the rebuttal by companies.

Finally, the role of the compliance officer seems underutilised so far. The DSA has undoubtedly influenced the internal structure of companies. However, the strong position of compliance officers in the internal governance structure should be better mapped and understood. Governance can act as an important facilitator of further compliance by persuasion.

The censorship critique

The DSA is a pioneering piece of legislation that tries to marry the risk-based approach with the regulation of digital services that often implicate the political liberties of individuals, such as freedom of expression. While the DSA tries to *advance* the rights of speakers by giving them procedural rights against private power that distributes their content, it also creates tools to *suppress* the distribution of illegal content or the proliferation of illegal behaviour. Thus, it both advances but also limits the freedom of expression.

The DSA does not create new content rules for users, that is, rules about what can be said by users online. The DSA does not even include an obligation to remove illegal content; but, by virtue of its liability exemptions, it offers an important incentive to remove manifestly illegal content.[90] The power to decide about content policy remains in the hands of parliaments, especially national parliaments, *and* in the hands of platforms that enjoy contractual freedom. In this sense, the DSA is an extra layer of tools for victims, civil society and the state to enforce regular norms on illegality. It is also confirmation of the contractual freedom of providers to set their own policies as they see fit if they respect local rules about illegality.[91]

[89] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) [2024] art. 18, Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024], art. 13 and 15.

[90] Digital Services Act, art. 6.

[91] Ibidem, art. 14(4); see Raue and Hoffman (n 40), art. 14.

The DSA thus only enforces what is already the law in the Member States.

The criticism of the DSA on the freedom of expression grounds comes from three main directions. First is the narrative that simply regulating social media is equivalent to censorship. Second is that enforcing hate speech rules is a form of censorship. Third is a more pointed critique that trying to suppress, or disincentivise disinformation might endanger legitimate speech, including by invoking the notion of "harmful but lawful content."

Regulating social media undoubtedly has a freedom of expression dimension. The highest courts of EU/US legal systems have been grappling with the constitutional limits of the legislative power.[92] However, while both systems draw the line between what is possible differently, owing to different legal traditions, neither system simply considers any regulation of social media censorship.

While extreme forms of imposition of liability on digital services can indeed inflict high levels of collateral censorship, as companies would remove content out of caution, the DSA preserves the liability exemptions that prevent this. If anything, the DSA protects against overreach by imposing liability on providers who are not aware of specific unlawful content.

The alleged intentional censorship of conservative voices by Big Tech has clear antidotes in solutions like those offered by the DSA – actionable transparency and procedural safeguards in favour of users. But in the general narrative of the second Trump administration, those safeguards for users are also being dismissed as censorship. In other words, it seems like the EU legislature must be damned if it tries to hold to account, but also if it fails to do so.

The criticism about the enforcement of hate speech rules has little to do with the DSA itself. Hate speech rules have a long tradition in Europe.[93] They were created by democratically adopted laws. The US, EU, and other regions differ on what types of speech are considered illegal under the rubric. But tech companies routinely resolve these differences by enforcing their own contractual rules, and then localising compliance with illegal content. Thus, unless the specific national law seeks extraterritorial effect, which is in itself controversial, the EU hate speech rules do not limit the speech of Americans in the US. If they do, it is usually the choice of companies who extend bans on such content to other countries.

---

[92] *Reno v. ACLU*, 521 U.S. 844 (1997); *Delfi AS v. Estonia* App. No. 64669/09 (Jun. 16, 2015); *Magyar Jeti ZRT v. Hungary* App. No. 11257/16 (Dec. 4, 2018), *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* App. No. 22947/13 (Feb. 2, 2016); *Sanchez v. France* App. No. 45581/15, (Sept. 2, 2021).

[93] Jacob Mchangama and Natalie Alkiviadou, 'Hate Speech and the European Court of Human Rights: Whatever Happened to the Right to Offend, Shock or Disturb?' (2021) 21(4) Human Rights Law Review; Mario Oetheimer, 'Protecting Freedom of Expression: The Challenge of Hate Speech in the European Court of Human Rights Case Law Symposium: Comparative Law of Hate Speech' (2009) 17 Cardozo J Int'l & Comp L 427.

European hate speech laws[94] have been subject to an ongoing debate that is entirely legitimate. However, only because Europeans have different views than the US does not mean any side is wrong. In any case, the debate has little to do with the DSA itself because it does not create new content rules.

A related controversy pertains to trusted flaggers. In some member states, the concern has been that these organisations can remove content directly. Providers are not obliged to take down material notified by trusted flaggers. The certification of trusted flaggers only relates to illegal content. Thus, providers can reject their notifications if they are incorrect. In fact, the DSA only forces companies to receive more notifications from such entities but does not go as far as to say that companies must trust them and remove content automatically. If the removal is automatic then this is something that companies decided to do voluntarily, which they could have done even before the DSA, and with much less oversight. If anything, the DSA creates a framework for oversight of such actors and discourages incorrect notifications (Article 23).

Finally, as noted above, the third argument relates to the potential abuse of law in efforts against disinformation or harmful content. Disinformation as a legal concept does not exist in the DSA. However, it is often used as an umbrella term to deal with various phenomena, ranging from benign and lawful to very serious and unlawful. Harmful content only has a specific legal meaning with respect to minors (see below).

Even though the DSA does not create new content rules, and remains content-neutral, it has two provisions that could challenge this characterisation: Article 14(4) and Article 35. The former obliges providers to consider the fundamental rights of others when designing their content policies for users. If such content policies are disproportionate, they could be viewed by courts and regulators as illegal, and thus not a valid part of their mutual contract.

However, Article 14(4) must respect contractual freedom of companies. Thus, it is more likely that it can be invoked for content-neutral assessment of terms, such as lack of some procedural safeguards, or excessiveness of penalties, etc. Asking for content-specific restrictions based on Article 14(4), such as banning some lawful disinformation, should have the same problems as similar efforts under Article 35 (or possibly Article 28).

Article 35 obliges VLOPs and VLOSEs to mitigate risks arising from the use, functioning and design of their service. Some are of the view that the provision could serve as a basis for the regulator to regulate specific content, such

[94] Recommendation CM/Rec(2022)16[1] of the Committee of Ministers to member States on combating hate speech (Adopted by the Committee of Ministers on 20 May 2022 at the 132nd Session of the Committee of Ministers).

as disinformation.[95] The censorship argument usually invokes Article 35(1)(b) and the fact that the DSA covers also risks posed by otherwise lawful behaviour or expression into its scope.

As I have argued in another article and book,[96] I consider such reading not only a dangerous overreach of administrative authorities, but also against the legislative intent, and broader human rights constraints of the DSA. While it is true that the DSA's scope includes risks posed by otherwise lawful behaviour, there is also no provision in the DSA empowering the administrative authorities to impose new binding content rules for users through their supervision of online platforms.

Responsible Commissioner Henna Virkkunen recently affirmed the content-neutrality in a letter to United States House Judiciary Chair Jim Jordan. According to Politico, she wrote that the Digital Services Act (DSA) is "content-agnostic" and that Brussels and national regulators "have no power to moderate content or to impose any specific approach to moderation."[97]

The reference to terms and conditions (Article 35(1)(b)) can be seen as a reference to content-neutral adjustments, such as reformulation for the purposes of clarity, or compliance with precision and fairness requirements (Article 14(1) or (4)). In the legislative process, Commissioners have repeatedly confirmed that the law is "content-neutral."[98] Article 35 can hardly serve as a sufficient legal basis to impose restrictions on specific expressions of users because such restrictions would not be prescribed by the law. Thus, if interpreted correctly, in my view, neither Article 14(4) nor Article 35 should challenge the characterisation that the DSA does not create new content rules and remains content-neutral. But the truth remains that a stronger statement to this effect in the law itself would have been beneficial.

Finally, some point to the use of the term "harmful content" by media and regulators. The DSA does not recognise any special category of "harmful content." The term only has legal relevance in the context of audiovisual media law where it defines what content minors should not be able to see.[99] For the

---

[95] The study has been prepared by Reset but commissioned by Directorate-General for Communications Networks and Content and Technology (European Commission), see 'Digital Services Act: Application of the risk management framework to Russian disinformation campaigns' (2023), https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1/language-en

[96] Husovec, *Principles of the Digital Services Act* (n 6); Martin Husovec, 'The Digital Services Act's red line: what the Commission can and cannot do about disinformation' (2024) 16(1) Journal of Media Law 47.

[97] Politico, 'EU social media law isn't censorship, tech chief tells US critic' (10 March 2025), https://www.politico.eu/article/social-media-law-does-not-regulate-speech-eu-tech-chief-tells-us-lawmaker-henna-virkkunen/?ref=everythinginmoderation.co

[98] Husovec, *Principles of the Digital Services Act* (n 6), 334 ff.

[99] Article 6a of the Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions

purposes of the DSA, such regulated content is not easy to classify. It often involves content that is perfectly lawful but should not be shown to minors on some platforms. According to Article 3(h) DSA:

> "illegal content" means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.

Regulated content harmful to minors might be seen as information that is not in compliance with audio-visual media laws if they are shown to minors. It depends on how these categories are operationalised in the national law. Alternatively, it can be seen as a self-standing obligation of some providers. In any case, there is no comparable category for adults in the same audio-visual media laws. Plus, the category does not apply to all online platforms.

To use the concept along with illegal/unlawful content is therefore incorrect. Either the content is regulated on the basis of law, or it is not. There is nothing in between. This is why it was problematic when the former Commissioner, Thierry Breton, often used the term along with the term illegal content. In his letter to X/Twitter, he stated (emphasis mine):[100]

> This notably means ensuring, on one hand, that freedom of expression and of information, including media freedom and pluralism, are effectively protected and, on the other hand, that all proportionate and effective mitigation measures are put in place regarding the amplification of *harmful content* in connection with relevant events, including live streaming, which, if unaddressed, might increase the risk profile of X and generate detrimental effects on civic discourse and public security. This is important against the background of recent examples of public unrest brought about by the amplification of content that promotes hatred, disorder, incitement to violence, or certain instances of disinformation.

European civil society rightly criticised this choice of words and a broader approach.[101] Even the College of Commissioners distanced itself eventually from Breton's PR stunts.[102]

The best way that the Commission could handle the censorship criticism would be to issue specific public guidance that provides the interpretation of Articles 14(4) and 35 that firmly rejects the existence of any competence to create

---

laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities OJ L 303/69.

[100] Thierry Breton, (*X* 12 August 2024), https://x.com/ThierryBreton/status/1823033048109367549

[101] The Future of Free Speech et al., 'Open Letter to Thierry Breton on The DSA's Threats to Free Speech' (21 August 2024), https://futurefreespeech.org/open-letter-to-thierry-breton-on-the-dsas-threats-to-free-speech/

[102] Financial Times, 'Brussels slaps down Thierry Breton over 'harmful content' letter to Elon Musk' (13 August 2024), https://www.ft.com/content/09cf4713-7199-4e47-a373-ed5de61c2afa

new content rules by means of content-specific measures. Such guidance would draw a red line around the Commission's exercise of the powers. It could be accompanied by a commitment to always explain how enforcement actions on the basis of Articles 14(4) and 35 comply with this red line. Going forward, such explicit safeguards should be explicitly enshrined in the DSA itself.

Admittedly, the DSA should have been more explicit in legislating this safeguard. However, the oversight can still be remedied by the Courts that would eventually review any enforcement decisions that the Commission makes.

Private enforcement

The DSA has three provisions foreseeing some kind of private enforcement. Similarly as DMA, it submits the entire regulation to the collective enforcement regime of the Representative Actions Directive that grants collective redress to qualified consumer organisations (Article 90). Moreover, Article 54, introduced in the legislative process, foresees the possibility of damages for violations of the DSA. Finally, Article 86 gives user groups a right to represent users concerning their rights derived from the DSA.

The first months of application show that private enforcement will make an important contribution to DSA compliance. At the time of writing, I am aware of the following cases:

- A Dutch case concerning X/Twitter and shadow banning,[103]
- German pre-trial enforcement by a German association, Wettbewerbszentrale, concerning Temu and Etsy and their compliance with consumer obligations of online marketplaces (know your customer),[104]
- Italian cases by TikTok and Meta seeking review of AGCOM decisions in consumer law that allegedly violate the exclusive competencies of the European Commission,[105]
- A German case concerning X/Twitter and its compliance with data access provisions for researchers under Article 40(12) DSA,[106]

[103] Paddy Leerssen, 'The DSA's first shadow banning case' (*DSA Observatory* 6 August 2024), https://dsa-observatory.eu/2024/08/06/the-dsas-first-shadow-banning-case/

[104] Wettbewerbszentrale, 'DSA proceedings: TEMU undertakes to refrain from' (12 September 2024), https://www.wettbewerbszentrale.de/dsa-verfahren-temu-verpflichtet-sich-zur-unterlassung/; Wettbewerbszentrale, 'Competition authority sues Etsy' (8 April 2024), https://www.wettbewerbszentrale.de/wettbewerbszentrale-klagt-gegen-etsy/

[105] AGCOM, [press release] 'Tutela dei minori, agcom fa rimuovere diversi video sulla piattaforma TikTok' available at https://www.agcom.it/sites/default/files/migration/article/Comunicato%20stampa%2016-02-2024.pdf; Delibera 204/23/CONS, available at https://www.agcom.it/provvedimenti/delibera-204-23-cons.

[106] Daniel Holznagel, 'Berlin court rules on Art. 40(12) DSA – with broader lessons for private enforcement of the DSA, (*ottoschmidt* 12 February 2025), https://www.otto-schmidt.de/blog/it-recht-blog/berlin-court-rules-on-art-40-12-dsa-with-broader-lessons-for-private-enforcement-of-the-dsa-ITBLOG0007850.html

- An Irish case initiated by X/Twitter against the Irish Online Safety Code, an implementation of the Audiovisual Media Services Directive, as potentially pre-empted by the DSA.[107]

Of the above, the last two X/Twitter cases raise fundamental legal questions. The Irish and Italian case raises the questions of pre-emption by the DSA, and content-neutrality, while the German case direct enforceability of Article 40(12) and interaction of national courts with the Commission under Article 82(3) DSA (c.f. Article 39(5) DMA).

Since the Commission's preliminary findings against X relate also to Article 40(12), this would suggest that finding against X/Twitter should not create any obstacle to the issuance of an injunction. However, the opposite outcome could lead to questions of potential conflict with the Commission's view under the second sentence, and if the Commission adopts the non-compliance decision, also with the first sentence. In such a case, the German court could seek preliminary reference to the Court of Justice of the European Union.

Finally, as shown by the national reports, Member States have different confidence concerning the future of private enforcement of the DSA. However, several seem to be of the view that the most likely private enforcement will come from consumer organisations according to Article 90.

In this context, it is interesting to note that the majority of the Member States repealed their implementations of Articles 12-15 of the E-Commerce Directive (Austria, Denmark, Germany, Lithuania, Netherlands, Romania, Slovakia, Slovenia, Sweden). This often included also extended liability exemptions to other services, such as search engines.

Conclusions and recommendations

The DSA has the potential to reduce the opacity of central decision-making of platforms and increase the safety of users on digital services. Some of the envisaged effects are clearly materialising, while others might take a few more years to fully manifest themselves.
The DSA has a review clause in Article 91 which pays special attention to the impact on SMEs, competitiveness, and scope of regulated services. While the DSA is asymmetric, as noted above, the Commission should consider a number of areas where the DSA might be overly bureaucratic or less favourable for SMEs. I recommend several changes, most of which would improve the situation of SMEs. I explain some of them in more detail below.

- The Commission should have stronger investigatory powers for the purposes of Article 24(2) even before the companies are designated.

[107] Breakingnews.ie, ' 'X' asks High Court to quash Coimisiún na Meán decisions' (16 December 2024), https://www.breakingnews.ie/ireland/x-asks-high-court-to-quash-coimisiun-na-mean-decisions-1708506.html

The powers envisaged in Article 24(3) are very limited given Articles 56(2) and (3).

- The DSCs might consider maintaining voluntary registries of online platforms.
- The Commission should explore the designation of advertising services under the DSA.

Many advertising services constitute online platforms because they store and publicly disseminate other ads of advertisers. Since the definition of monthly active users extends to any user "exposed" to information posted by users, this includes also not only advertisers but also viewers of ads.[108]

- The Commission should empirically interrogate if incentives granted to trusted flaggers, out-of-court dispute settlement bodies, and user groups are always strong enough, and, possibly, if they are not too strong in some cases.
- The Commission, DSCs and companies should initiate a close mapping of the terms and conditions violations against the illegality rules in the EU Member States.

As explained above, such mapping would allow companies to continue deciding against their own terms and conditions, and to keep one main channel for notifications, but would improve the application of provisions of the DSA that are specifically targeting illegal content.

- The European Commission should invest resources in facilitating de facto standardisation of many practical questions of cooperation between out-of-court dispute settlement bodies and online platforms.

Such standardisation can lower the overall costs of the system but also encourage entry by new ODS bodies. As explained earlier, there are a number of issues that require coordination.

- The Commission should study the impact of the out-of-court dispute settlement system (Article 21) on companies (and users), especially whether, given the dominant financing structure, it should extend to all online platforms regardless of their importance.

While ODS bodies are themselves opting to cover mostly the most popular services, which somewhat mitigates the impact on mid-sized online platforms, the problem might still arise in the future. One simple solution would be to adjust the financing system for non-VLOP/VLOSE providers, where the complainants would have to always initially pay the full overall fee, which would be reimbursed upon success.[109] Special attention should be also paid to linguistic coverage across the EU.

---

[108] For a discussion, see Pieter Wolters and Frederik Zuiderveen Borgesius, 'The EU Digital Services Act: what does it mean for online advertising and adtech?' (2025), https://arxiv.org/abs/2503.05764

[109] This was the original design proposed by Lenka Fiala and Martin Husovec, 'Using experimental evidence to improve delegated enforcement' (2022), 71 International Review of Law and Economics.

- The language for audit results seems misleading. The Commission should encourage complementary language by auditors, such as "overall positive," or "predominantly positive," or in percentage.
- The Commission should closely map the position of compliance officers in the internal governance structures of companies.
- The EU legislatures should clarify that nothing in the DSA can serve as a legal basis to impose obligations on providers to prohibit or otherwise limit specific expressions of their users that are lawful under the law. In the meantime, the Commission should adopt a guidance that draws a red line around the Commission's exercise of its powers. The guidance could be accompanied by a commitment to always explain how enforcement actions on the basis of Articles 14(4), 28 and 35 comply with this red line.
- The DSA should clarify that on composite services, such as social media, only central decision-making by the overall provider is subject to any due diligence obligations. Thus, owners of pages or groups on major social media services should not fall under the hosting due diligence obligations, but can still benefit from the liability exemptions.
- The Commission should analyse whether the benefits of the statement of reasons database (Article 24(5)) are justified by its costs for non-VLOPs/VLOSEs.[110]
- The Commission should explore whether the enhanced obligations for VLOPs/VLOSEs need to remain the same regardless of the track record of regulatees over the years.

To motivate companies, the DSA might borrow the mechanism of suspension from the DMA (see Article 9). The possible options could be to suspend the application of selected provisions in the VLOP/VLOSE tier, such as audits or prolong the risk assessment cycle. VLOPs/VLOSEs anyway remain subject to an obligation to produce ad hoc off-cycle risk assessment whenever they introduce features that can have a critical impact on their risk profile (Article 34(1)).

- The Commission should consider internal differentiation of VLOPs, for instance by user count, because the designation under the DSA is becoming increasingly used in other acts of EU law as a shorthand for Big Tech, which does not always reflect their internal diversity.[111]
- The future update of the DSA should harmonise the questions of issuance of cross-border orders, their follow-up enforcement, EU-wide effects, and safeguards.

[110] On VLOPs/VLOSE, researchers have already used the data to gain many, and their findings point to many useful insights. See Daria Dergacheva et al., 'One Day in Content Moderation: Analyzing 24 h of Social Media Platforms' Content Decisions through the DSA Transparency Database' (2023) Center for Media, Communication, and Information Research (ZeMKI).

[111] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) [2024] art. 18, Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024], art. 13 and 15.

Orders issued by authorities are not properly regulated by the DSA. There was a lack of political will to do so. This is now felt by the DSCs and other national authorities who continue to struggle with the enforcement of their domestic orders. Articles 9-10 that create a feedback mechanism are not sufficient. The problem is compounded by a lack of clear rules about cross-border enforcement of administrative orders, or better rules on cross-border enforcement of judgments. This gap was known at the time of the legislative process, but Member States were not willing to go beyond the status quo.

An ideal future update of the DSA would supplement Articles 9-10 with a universal list of safeguards, and rules on cross-border competence and enforcement. Such effort could also try to codify the case law on what constitutes specific monitoring allowed by Article 8 because there continues to be a lot of divergence in how some courts understand the concept. The EU legislature should pay special attention to orders that are based on local competence but might have EU-wide validity (e.g., blocking of violent hate speech).

- The future update of the DSA should better incentivise content creators whose content is widely praised for its high quality.

The DSA does not regulate content creators. Thus, Member States are free to develop rules about influencers and similar superusers, as long as they do not regulate platforms. While such subject matter arguably falls outside of the scope of the law, the DSA could consider mechanisms that incentivise better organisation of content creators who produce high-quality content. At the moment, the DSA grants the same procedural rights to everyone, regardless of their track record or history. As I have argued elsewhere,[112] such a starting point is understandable, but should not stop us from giving better treatment to those who have a strong track record of high-quality content. European Media Freedom Act's attempt to do so for media service providers, unfortunately, does not sufficiently link new privileges with the track record and looks more at the status of legacy media, although it is preconditioned on some form of independence.[113] This could be also achieved through Codes of Conduct.

- Stakeholders and regulators must continue working on increasing the awareness among those who are empowered by the law.

Section 3: Digital Markets Act

The Digital Markets Act is a collection of prescriptive rules inspired by controversies of competition law enforcement against tech companies over the last two decades. The DMA only targets powerful actors that act as a bottleneck for business users.

[112] Martin Husovec, 'Trusted Content Creators' (2022), LSE Law - Policy Briefing Paper No. 52.
[113] European Media Freedom Act (n 109), art. 17.

Once the "gatekeepers" are designated by the European Commission, they become subject to numerous per se obligations. The common declared goal of these obligations is to increase fairness and contestability of the underlying markets.

Two leading competition scholars, Pierre Larouche and Alexander de Streel eloquently summarize the DMA's contribution as follows:

> While the DMA will be a revolution in Big Tech regulation, it is mostly built on traditional policy choices which have been made before in other EU economic regulatory frameworks. Indeed, the DMA is a regulatory tool that will complement competition law, although it is positioned somewhat uncomfortably between the two, in epistemological terms. It aims at opening paths for sustaining and disruptive innovation. It foresees mostly behavioural interventions leaving structural interventions for very exceptional circumstances. It relies on detailed rules that are easier to enforce than flexible standards. Only one choice is truly path-breaking, and that is to favour centralised enforcement through the Commission over decentralised enforcement by national independent authorities.[114]

In their article, the two authors present the view that a stronger case for the DMA is in supporting users' innovation who often innovate by introducing complementary products for the gatekeepers' ecosystem (e.g., apps, or features).[115] I fully agree that this type of innovation arguably constitutes the primary focus of the law. As noted in the introduction, the DMA rather *recalibrates* the ability of companies to appropriate their investments.[116] It puts some limits on how they can exploit their ecosystems in the pursuit of profit by giving some affordances to users and banning some practices. This improves the "sustainability of innovation" by users of such ecosystems.[117] The key mechanism for this is potentially increased appropriability of investments of business users. Such innovation is mostly of incremental type which, however, equally contributes to consumer welfare and innovation trajectories.[118]

In contrast, the theory behind the DMA incentives for disruptive innovation is that it might make the position of core platform services more contestable by weakening their entrenchment. Pierre Larouche and Alexander de Streel argue that some DMA obligations, such as advertising transparency, data portability, or bans on Most Favoured Nation (MFN) clauses or anti-steering provisions, could increase the vulnerability of providers to disruption.[119] Thus, the DMA "opens a path to disruption."[120] Ibáñez Colomo sees it most clearly in the DMA's attempts to force companies to open up their core segments by

[114] Larouche and de Streel (n 30) 560.
[115] Ibidem, 549 and 551.
[116] Ibáñez Colomo (n 30) 145.
[117] Larouche and de Streel (n 30), 549; Ibáñez Colomo (n 30) 144.
[118] Larouche and de Streel (n 30), 549.
[119] Ibidem, 550.
[120] Ibidem, 551.

opening up closed parts of the value chain to third-parties via interoperability, such as that of competing messaging services.[121] While such interventions are certainly important and more interventionist than others, arguably, compared with the DMA's contribution to complementary innovation, its likely contribution to contestability is going to be more modest.

Looking at the DMA's architecture, we observe several types of obligations whose rationale is somewhere on the spectrum between the stated goals of fairness and contestability.

Some obligations try to outlaw more aggressive business-to-business practices, such as insider imitation of products by gatekeepers (Article 6(2)), self-preferencing (Article 6(5)), and practices that prevent business users from developing their businesses on their own terms (many in Article 5). Others intervene to increase the contestability of the CPS services in the core market segment, such as interoperability obligations for messaging apps (Article 7). The main common denominator of rules, however, is arguably the attempt to achieve fairness and contestability through better empowerment of business users and end users.

To do this, the DMA grants users new agency to change defaults on software applications (Article 6(3)), install and switch new apps or entire app stores (Articles 6(4), 6(6)), interoperate with gatekeepers' hardware and software (Article 6(7)), including competing messaging services (Article 7), and port users' data (Articles 6(9) and 6(10)), and object to combination of personal data by gatekeepers (Article 5(2)). The empowerment mechanism is thus meant to shake things up by giving better choices to users. However, it also means that if users' choice is something that will not materialise in practice, many of the expected benefits will not either.

The DMA's scope and designation of gatekeepers

To date, the European Commission has designated 7 gatekeepers for 24 core platform services (CPSs).[122] As Commission officials themselves have acknowledged,[123] there have been some challenges in defining the boundaries of the core platform services – making this process arguably more complex than expected.

[121] Ibáñez Colomo (n 30) 136.

[122] See European Commision, 'Gatekeepers' https://digital-markets-act.ec.europa.eu/gatekeepers_en.

[123] Alberto Bacchiega & Thomas Tombal, 'Agency Insights: The first steps of the DMA adventure,' (2024) 12(2) Journal of Antitrust Enforcement, 191–192.

Figure 8. Gatekeepers under the DMA

	Gatekeepers						
	Alphabet	**Amazon**	**Apple**	**Booking**	**Bytedance**	**Meta**	**Microsoft**
Core Platform Services	Googe Play	Marketplace	AppStore	Online intermediation services	TikTok	Facebook Marketplace	LinkedIn
	Google Maps	Amazon Advertising	iOS			Facebook	Windows PC OS
	Google Shopping		Safari			Instagram	
	Google Search		IPadOS			WhatsApp	
	Youtube					Messenger	
	Android Mobile					Meta Ads	
	Alphabet's online advertising						
	Google Chrome						

For instance, questions arose about the type of CPS offered by a particular gatekeeper (whether TikTok is a video-sharing service or an online social network) and whether a specific functionality offered by a gatekeeper qualifies as a separate service or an integral part of the CPS.[124] So far, the DMA designation process appears to be working reasonably well and is effective in identifying the market players and services relevant to protecting the contestability and fairness of markets in the digital sector – in line with the objective of the DMA in Article 1(1).

No gatekeepers have yet been designated for virtual assistants and cloud computing services as CPSs. More controversial, however, is the rise of another type of service that is not included in the DMA's list of CPSs, namely generative artificial intelligence (AI) systems. It is fair to say that the inclusion of AI systems in the list of CPSs would have been premature at the time of the adoption of the DMA. Although this means that AI systems currently cannot be regulated as a stand-alone CPS under the DMA, other CPSs already do or may at some point rely on large language models (such as search engines or social networks) and will then be covered, at least to some extent, by the DMA's substantive obligations. This allows the fitness of the DMA to be monitored in light of new developments and, if necessary, to rely on Article 19 DMA to add generative AI systems as a standalone CPS at a later stage.

The outcome of the designations shows that the DMA differs in approach from EU competition law. One illustration of this is that more than one gatekeeper has been designated for several CPSs (including for online social networks, operating systems, and online advertising services), while there can normally only be one dominant undertaking in a given relevant market under EU competition

[124] For an in-depth analysis of the delineation of core platform services, see Friso Bostoen & Giorgio Monti, 'The Rhyme and Reason of Gatekeeper Designation under the Digital Markets Act,' (2024) TILEC Discussion Paper No. 2024-16, 3-11, available at http://dx.doi.org/10.2139/ssrn.4904116

law. The General Court also clearly sets the DMA apart from EU competition law in its judgment dismissing Bytedance's appeal against the Commission's decision to designate Bytedance as a gatekeeper with TikTok as CPS.

In sketching the context of the DMA, the General Court recalled the EU legislature's belief that "existing EU law did not address, or did not address effectively, the challenges to the effective functioning of the internal market posed by the conduct of gatekeepers that are not necessarily dominant in competition law terms" and that "the DMA pursued an objective that is complementary to, but different from, that of protecting undistorted competition on any given market, as defined in competition law terms."[125]

While Bytedance relied on case law in the domain of EU competition law and state aid to claim that it should be allowed to deliver new arguments or evidence for the first time before the Court, the General Court argued that this case law "concerns legal frameworks and fields of law which are different from those covered by the DMA" and therefore does not apply.[126]

Moreover, the General Court refused to interpret the concept of "entrenched and durable position" for gatekeeper designation in line with the notion of dominance under Article 102 TFEU on the ground that "the EU legislature knowingly chose to use a new concept, different from that of 'dominant position.'"[127] For the DMA to achieve its objective, its interpretation and enforcement should not mimic approaches from EU competition law – even though some of the investigative powers under the DMA are modelled on those of Regulation 1/2003.

These explicit statements by the General Court are therefore welcome and will contribute to the effectiveness of the DMA as a complement to, rather than a substitute for, EU competition law. TikTok appealed the judgment of the General Court.[128]

Many designation disputes are motivated by more than mere judicial review of the designation decisions itself. In *Apple v Commission*,[129] for instance, Apple is also seeking an incidental review of the constitutionality of Article 6(7) on the basis of the Charter of Fundamental Rights. This shows why the involvement of civil society (Free Software Foundation Europe (FSFE)), and stakeholder representatives (Coalition for App Fairness)[130] is key because these cases are about much more than narrow designation questions.

---

[125] Case T-1077/23 *Bytedance v European Commission* [2023] ECLI:EU:T:2024:478, para 19.

[126] Ibidem, para 234-237.

[127] Ibidem, para 298.

[128] Case C-627/24 P *Bytedance / Commission* [2024].

[129] Case T-1080/23 *Apple v Commission* [2023].

[130] Order of the President of the Eight Chamber, August 1, T-1080/23, accepted Coalition for App Fairness and Free Software Foundation Europe as interveners on the side of the European Commission. See my disclosure on page 1. I represent FSFE as an intervener in the General Court.

Substantive obligations

The DMA imposes a range of obligations and prohibitions on gatekeepers in Articles 5, 6 and 7. Compliance with all obligations and prohibitions is required, but it is not feasible to monitor all of them at the same time. It is therefore necessary to set good priorities as to how enforcement resources are to be allocated. Two and a half weeks after the compliance deadline, the European Commission opened five non-compliance investigations against Alphabet, Apple and Meta in March 2024.[131]

Arguably most important for the DMA to achieve its objectives of contestability and fairness is to protect the openness of digital ecosystems. In this light, the non-compliance investigations can be said to focus on the right priorities by looking into:

(1) Apple's and Alphabet's compliance with the anti-steering prohibition in their app stores,[132]
(2) concerns about Alphabet favouring its own vertical search services over competing services,[133]
(3) Apple's presentation of web browser choice screens,[134] and
(4) Meta's pay or consent model to comply with the DMA's requirement to obtain consent from users in order to combine or cross-use personal data.[135]

At the same time, there are other obligations and prohibitions that have not yet been the subject of investigations but are important too.[136]

The European Commission holds the exclusive power to enforce the DMA. Thus, combining available resources and involvement of NCAs is recommended to ensure as effective and as complete compliance as possible. Moreover, private enforcement can be a key additional channel that will allow the business community to push compliance on the issues where the Commission might have little, or opposite interests. Most national rapporteurs consider collective action the most promising avenue for private enforcement in the Member States.

Gaps in the DMA's architecture

The DMA includes a number of obligations that require companies to share data, interoperate, or facilitate interoperability. However, the law omits to

[131] European Commission, 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act,' (2024) available at https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en

[132] Digital Markets Act, art. 5(4).

[133] Ibidem, art. 6(5).

[134] Ibidem, art. 6(3).

[135] Ibidem, art. 5(2).

[136] This includes for instance the transparency requirements in online advertising services, namely Digital Markets Act, art. 5(9) and (10).

engage a broader set of stakeholders around such exercises. Unlike under the DSA's Article 40, in the absence of further specification by the regulator, the companies are fully left in charge of deciding the scope of these obligations. Going forward, the DMA would benefit from the creation of a broader ecosystem that would support companies' compliance efforts, particularly around questions such as portability, interoperability and data sharing. Professional organisations in a particular area, or consumer organisations, could become useful partners for companies when trying to reconcile the conflicts between the empowerment of users, and the security or the integrity of their systems, including the protection of necessary trade secrets. Inevitably, many of these conversations will be extremely technical, which is why standardisation (Article 48), and other voluntary consensual stakeholder exchanges should be encouraged by the Commission.

The obvious candidates for these efforts are the issues of interoperability of messaging systems (Article 7), apps and app stores (Articles 6(4) and (7)), and facilitation of third-party content moderation services on social media via middleware services (Articles 6(7) and 6(10)).

Public and Private Enforcement

The EU legislator distinguished the obligations of Articles 6 and 7 DMA as "susceptible of being further specified" from those of Article 5 DMA that are not susceptible of further specification in a dialogue with the respective gatekeeper.[137] Experience to date shows that the obligations contained in both Article 5 and Article 6 of the DMA may require further interpretation, as non-compliance investigations cover both provisions and address the extent to which current actions of gatekeepers are sufficient to meet the requirements.

Figure 10. Pending DMA investigations

Types of obligation	Alphabet	Meta	Apple	Amazon
Personal Data		5(2)*		
Promotion of offers by business users	5(4)		5(4)*	
Users un-installing applications and changing default settings			6(3)	6(5)
Users installing third-party applications			6(4)	
Ranking	6(5)			6(5)

* *Note.* After the report was finalised, the Commission issued non-compliance decisions in these two cases.

The Commission is also defending four of its designation decisions before the Court of Justice of the European Union: *Bytedance v. Commission* C-627/24 P,[138]

[137] See also Digital Markets Act, Recital 65.

[138] General Court case: T-1077/23; Interim measures: T 1077/23 R.

Meta v. Commission T-1078/23, s*Opera Norway v. Commission* T-357/24, and *Apple v. Commission*, T-1080/23. TikTok's and Meta's cases concern the appropriateness of designation. Apple's case, as noted above, in addition challenges the validity of Article 6(7) of the DMA.[139]

Figure 11. Pending DMA disputes before the CJEU

Reasons for action	T-1077/23 Bytedance v. Commission	T-1078/23 Meta v. Commission	T-357/24 Opera Norway v. Commission	T-1080/23 Apple v. Commission
Contestation of designation	3(1), (5)	3(9)		3
Contestation of failure to designate			3(1), (4), (5)	
Validity of obligation imposed by DMA				6(7)

While efforts have been made to categorize the range of obligations and prohibitions according to different "theories of harm,"[140] it is difficult to identify one uniform underlying set of principles or beliefs. The objectives of contestability and fairness can, to some extent, guide the interpretation of unclear aspects of the DMA obligations, but in many cases, the two objectives do not prescribe one particular outcome.[141]

Private enforcement can be especially useful to ensure compliance with obligations that contain open or unclear terms and are not yet taken up by the Commission in ongoing non-compliance investigations. The DMA foresees cooperation mechanisms with national courts to ensure its coherent application. This includes the possibility of the Commission submitting observations to national courts and the requirement of national courts to refrain from delivering a judgment running counter to a Commission decision or conflicting with a decision contemplated by the Commission in proceedings it has initiated under the DMA.[142]

With these cooperation mechanisms in place, private enforcement is a valuable complement to public enforcement by the Commission. A challenge for claimants in private cases will be to prove and quantify their damages as well as to demonstrate that the damages were caused by an infringement of the DMA. Stand-alone cases can be particularly challenging, as claimants must also prove that the DMA has been breached – whereas information to establish such a violation may not be readily available and only be in the hands of

[139] See *Case T-1080/23 Apple v Commission* [2023].

[140] For instance, see the four categories identified by CERRE: (1) preventing anti-competitive leverage from one service into another, (2) facilitating switching and multi-homing for both business and end-users, (3) opening platforms and data, and (4) increasing transparency. Alexandre de Streel et al., 'Effective and Proportionate Implementation of the DMA,' (2023), 32, available at https://cerre.eu/wp-content/uploads/2023/01/DMA_Book-1.pdf

[141] As defined in Digital Markets Act, Recitals 32 and 33.

[142] Respectively, Digital Markets Act, art. 39(3), (4) and (5).

the gatekeeper or the relevant authorities. Another aspect that may discourage claimants from bringing private actions is the so-called "fear factor." Those who are harmed by a gatekeeper's behaviour are also often dependent on it to reach customers or generate revenue and may be concerned that the gatekeeper will react by implementing even more restrictive measures.

NCAs could play a role in addressing this fear of retaliation by acting as a first point of contact for businesses and consumers in their jurisdiction by receiving and investigating complaints and advising businesses and consumers on the next steps. This could include starting private litigation or bringing the case to the attention of the Commission. Even though NCAs do not hold any formal enforcement powers, they are an important actor in the DMA's institutional ecosystem.

Smaller or less experienced businesses and consumers are more likely to approach the respective authority in their jurisdiction than to immediately escalate a case to the Commission. The DMA also foresees in cooperation mechanisms between the Commission and NCAs to ensure "coherent, effective and complementary enforcement of available legal instruments."[143]

Noteworthy is that the DMA preempts the application of rules with a similar scope and underlying objectives at the national level.[144] This is important not only for the gatekeeper, who is now subject to a single EU regime, but especially for smaller business users who would otherwise have to navigate different legal frameworks across EU Member States. In this regard, it is also important for the Commission to closely monitor the developments regarding the introduction of a market investigation tool in several Member States (including Germany, Norway, Italy, Denmark).[145]

A market investigation tool allows a competition authority to intervene in a market to address a structural market problem without having to identify a violation of the competition rules. The tool is also referred to as the "New Competition Tool," as it was called when its introduction was considered as part of the Digital Services Act package in 2020.[146] The Draghi report has reopened the debate on the introduction of a New Competition Tool at the EU level.[147] Although the New Competition Tool does not directly interact with the DMA, some of the core platform services regulated under the DMA may also face structural market problems.

---

[143] Ibidem, art. 37 and 38.

[144] Ibidem, art. 1(5) and (6).

[145] Other EU Member States are also considering to introduce a market investigation tool. For a discussion of the Dutch context, see Jasper van den Boom et al., 'Towards Market Investigation Tools in Competition Law: The Case of the Netherlands,' (2023) 14(8) Journal of European Competition Law & Practice, 553–564.

[146] See the 2020 Impact Assessment for a possible New Competition Tool, available at https://competition-policy.ec.europa.eu/public-consultations/2020-new-comp-tool_en

[147] Draghi (n 35), Part B 303-304.

If different Member States have their own versions of a New Competition Tool, this could lead to diverging competences and market outcomes – if certain digital markets are regulated more strictly in one Member State than in others. While a degree of experimentation and divergence can sometimes be useful to learn and evaluate what approaches work, the coexistence of different regulatory frameworks and competencies risks fragmenting the internal market – which is arguably particularly problematic when dealing with powerful and global companies.

Conclusions and recommendations

The DMA is limiting the scope of business and design practices that can generate better profits for gatekeepers. It is thus understandable that it is resented by regulatees. However, claiming that the DMA is protectionist, or was adopted to extract extra revenue from the US companies, seems not very convincing if benefits are offered to all companies who conduct business via these services in the European Union.

In addition to the general recommendations mentioned above, I recommend the following:

- The Commission should facilitate the creation of informal institutions that would facilitate exchange on technical issues between companies and business users.

Very technical questions such as portability, interoperability and data sharing often require complex discussions that are not best suited to primarily regulatory fora. Professional organisations in a particular area of expertise could become useful partners for companies when trying to reconcile the conflicts between the empowerment of users, and the security or the integrity of their systems, including the protection of necessary trade secrets.

Inevitably, many of these conversations will be extremely technical, which is why standardisation (Article 48), and other voluntary consensual stakeholder exchanges should be encouraged by the Commission.

- The Commission should formally embrace the role of NCAs in filtering credible complaints where companies are justifiably afraid of retaliation.

NCAs could play a role in addressing this fear of retaliation by acting as a first point of contact for businesses and consumers in their jurisdiction by receiving and investigating complaints and advising businesses and consumers on the next steps.

- The EU legislature should further explore the need for a market investigation tool that allows a competition authority to intervene in a market to address a structural market problem without having to identify a violation of the competition rules.

From the internal market perspective, it is problematic if different Member States have their own versions of a New Competition Tool. Such a situation can lead to diverging outcomes if certain digital markets are regulated more strictly in one Member State than in others.

Comparative Report: Table of Contents

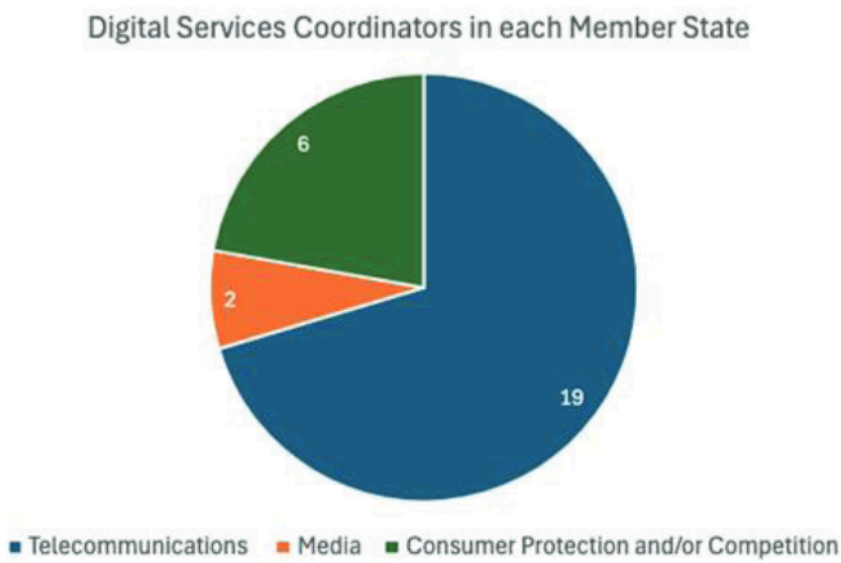
Section 1: National Institution Set-up

Question 1. Allocation of DSA competences

Which pre-existing or new authorities have been designed for the DSA enforcement in your Member State? If several, how are the tasks and responsibilities divided between them? How do such authorities interact with national sector-specific regulators (e.g., media, data protection, and consumer authorities)?

According to the reports, most of the Member States designated a telecommunications authority as their Digital Services Coordinator ("DSC"). The majority of the Member States also designated sector-specific authorities to ensure the protection of personal data, consumers, minors, or intellectual property, with only five Member States choosing to designate only a DSC.

While a few Member States have not yet decided on the division of responsibilities among the designated authorities, most national implementing acts provide for cooperation and guidance measures between the DSC and sector-specific authorities.



Sector-Specific Authorities' Competencies Following DSA Articles

	14	18	25	26	27	28	30	31	32	37	
Croatia					x	x					
Finland		x	x	x					x	x	
France			x	x		x	x	x	x		
Germany	x	x		x		x					
Lithuania	x		x	x	x		x	x	x		
Slovenia				x		x					
Spain				x		x					
Sweden	x	x	x	x	x	x	x	x	x	x	

	Digital Services Coordinator	Sector-specific authorities
Austria	Austrian Communications Authority ("KommAustria")	N/A
Belgium	Belgian institute for Postal Services and Telecommunications ("BIPT")	– Authorities designated for the 3 language -based Communities (Flemish, French, German): – Conseil Supérieur de l'Audiovisuel ("CSA") – Vlaamse regulator voor de media ("VRM") – Medienrat
Bulgaria[a)]	Commission for Regulation of Communications	Council for Electronic Media Commission for Data Protection
Croatia[b)]	Croatian Regulatory Authority for Network Industries (HAKOM) 5 other authorities (Art. 9 and 10 DSA)	Croatian Personal Data Protection Agency (Art. 27 and 28 DSA) 5 other authorities (Art. 27 and 28 DSA)
Czechia[c)]	Czech Telecommunication Office ("CTO")	Ministry of Industry and Trade and the Personal Data Protection Office ("PDPO") for personal data protection matters and coordination with other Member States
Denmark	Danish Competition and Consumer Authority	N/A

[a)] The bill amending the Bulgarian Electronic Communications Act has not been adopted as law yet.

[b)] The Act on the implementation of EU Regulation 2022/2065 has not been adopted yet.

[c)] The implementation of the DSA is not finished yet, as the Digital Economy Act has not been enacted.

Finland	Finnish Transport and Communications Agency Traficom ("Traficom")	Consumer Ombudsman (Art. 25, 26(1) a-c, 26(2), 37, and 32(7) DSA) Data Protection Ombudsman (Art. 26(1) a-d, 26(3), 27, and 28 DSA) Police (Art. 18 DSA) Market Court Legal Register Centre ("LRC")
France	Regulatory Authority for Audiovisual and Digital Communication ("Arcom")	Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF") (Art. 25 and 30 to 32 DSA) Commission Nationale de l'Informatique et des Libertés ("CNIL") (Art. 26(1) d, 26(3), and 28(2) DSA)
Germany	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways (BNetzA)	Federal Agency for the Protection of Children and Young Persons in the Media (Art. 14(3) and 28(1) DSA) Federal Commissioner for Data Protection and Freedom of Information (Art. 26(3) and 28(2)-(3) DSA) Federal Criminal Police Office (Art. 18 DSA) State authorities are responsible for content and diversity-related requirements
Greece	National Committee of telecommunications and post	Personal Data Authority for personal data protection matters (Art. 26(1)(d) and (3) and 28(1) DSA) National radio and television council for supervision of service providers (Art. 26(1)(a) to (c) and (2), and 28 DSA)
Hungary	National Media and Infocommunications Authority ("NMHH")	Hungarian competition authority ("GVH")
Italy	Authority for Communications Guarantees ("AGCOM")	Italian Competition Authority-Autorità Garante della Concorrenza e del Mercato ("ICA" or "AGCM") Data Protection Authority (Garante per la protezione dei dati personali)
Latvia	Consumer Rights Protection Centre (CRPC)	N/A

Lithuania	Communications Regulatory Authority ("CRA")	State Consumer Protection Authority (Art. 25, 26, 30, 31, and 32 DSA) State Data Protection Inspectorate (Art. 26(1) d, 28(2), and 27 DSA) Office of the Inspector of Journalistic Ethics (Art. 14.3 and 28(1) DSA)
Netherlands[d)]	Authority for Consumers and Markets ("ACM")	Dutch Data Protection Authority (Autoriteit Persoonsgegevens) (Chapter 3 DSA) Digital Regulation Cooperation Platform (Samenwerkingsplatform Digitale Toezichthouders) for coordination matters with other national authorities
Norway[e)]	Not designated yet	N/A
Poland[f)]	** Not officially designated yet Prezes UKE Urzędu Komunikacji Elektronicznej (Regulator for Electronic Communications)	** Not officially designated yet Prezes Urzędu Ochrony Konkurencji i Konsumentów UOKIK (the Polish Competition Authority)
Portugal	National Authority for Communications ("ANACOM")	Entidade Reguladora para a Comunicação Social - ERC (Regulatory Entity for Social Communication) for matters related to social communication and other media content IGAC (General Inspectorate for Cultural Activities) for copyright matters
Romania	National Authority for Management and Regulation in Communications ("ANCOM")	N/A
Slovakia	Council for Media Services (Rada pre mediálne služby)	N/A
Slovenia	Agency for Communication Networks and Services of the Republic of Slovenia ("AKOS")	Information Commissioner (Art. 26(1), 26(3), and 28 DSA)
Spain[g)]	National Commission for Markets and Competition (CNMC)	Still being discussed: – Data Protection Authority (Art. 26(3) and 28(3)

[d)] The DSA Implementation Act is currently pending before the House of Representatives.

[e)] The DSA is not yet applicable in Norway.

[f)] The act implementing the DSA has not been adopted yet.

[g)] The implementing legislation, Law on Information Society Services and Electronic Commerce/Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), was modified by the recent Royal Decree Law 9/2024. However, Royal Decree Law 9/2024 in turn has been repealed by a Congress Resolution of 22 January 2025. Nevertheless, it is expected that the legal changes introduced by Royal Decree Law 9/2024 will finally see the light of day very soon.

Sweden	The Swedish Post and Telecom Authority	The Swedish Consumer Authority (Art. 25, 26(1), 26(3), 27, 28(2) + 9-42 + 44, 45, 48 + 64, 66, 67, 69, and 72 DSA) The Swedish Agency for the Media (Art. 14, 25, 26(1), 26(2), 26(3), 28 + 11-42 + 44, 45, 48 + 64, 66, 67, 69, and 72 DSA)

Question 2. Special rules for DSA

Which specific rules, resources or other measures that have been adopted regarding the supervisory, investigative and enforcement powers of the competent authorities under the DSA? (e.g., allocation of powers and resources, the existence of special technical units, presence of procedural safeguards, supervisory fees, etc.) How many staff are dedicated to DSA enforcement?

Regarding staff resources, DSCs range between having two to seventy employees dedicated to the DSA, a few being the result of a new department or unit which was set up for the DSA. Nine Member States plan on hiring additional staff for their DSCs in the future.

Concerning financial resources, only Greece, Italy, and Romania answered positively in regard to the imposition of supervisory fees. The Romanian DSC will only start to impose such fees in 2027.

	Powers of Designated Authorities	Financial Resources	Staff Resources	Procedural Safeguards
Austria	KommAustria (DSC) can: – Decide on specific matters after having conducted an administrative procedure (Art. 54 and 51(3) DSA) – Impose fines and periodic penalty payments	KommAustria's federal budget is EUR 2,501,000 in 2024. No sector-specific funding provided for.	KommAustria has 6–7 full-time employees. Budget allows for hiring additional staff if necessary.	KommAustria must submit an application to the Federal Administrative Court to order temporary restriction of access to a provider (51(3) and 82(1) DSA).
Belgium	BIPT (DSC) is competent for: – Consumer protection – Price and income policy – Competition law – Trades and practices law	N/A	BIPT will have 22 full-time employees for the DSA. CSA does not currently have a team.	N/A

	– Commercial and company law – Residual competences (criminal and police matters) Communities authorities are competent for: – Providers of intermediary services that enable audio-visual media services – Protection of young people		VRM does not have additional full-time employees. Medienrat has 1 full-time employee for the DSA.	
Bulgaria	The bill makes reference to powers allocated under the DSA.	N/A	N/A	N/A
Croatia	HACOM (DSC) can: – Coordinate bodies (Art. 49(2) DSA) – Exercise powers based on Art. 51 and 53 DSA – Compile annual reports (Art. 55 DSA) – Cooperate with other Member States (Art. 58 DSA)	Government has the obligation to provide sufficient funds (unknown amount).	Currently, HACOM has several part-time employees. Full-time employees will be hired soon (number unknown).	N/A
	– Participate in the European Committee for Digital Services (Art. 62 and 63 DSA) – Exercise powers for out-of-court settlement disputes (Art. 21 DSA) – Exercise powers based on Art. 22 DSA			
Czechia	N/A	N/A	The proposal foresees that the CTO (DSC) will need up to 12 additional employees and the PDPO up to 2.	N/A

Denmark	N/A	The estimated budget is EUR 684,000 (to be evaluated in 2025). It will be evaluated whether supervisory fees are possible.	N/A	N/A
Finland	Traficom (DSC) can: – Conduct inspections and investigations – Order sanctions – Request access to an intermediary service to be blocked by a court – Assist the Commission (Art. 69 DSA) – Coordinate with other bodies – Supervise intermediary services (even if there are no VLOPs in Finland) Consumer Ombudsman's powers are broadened with the DSA in regard to: – Penalty payments – Art. 25 and 26 DSA	Traficom will require an additional budget of EUR 650,000. Consumer Ombudsman will require EUR 228,000.	N/A	N/A
France	Arcom (DSC) can: – Investigate – Collect necessary information (Art. 58 and 65 DSA) – Inspect service providers' offices – Require the service providers to cease any violation – Take corrective measures – Adopt provisional injunctions – Impose fines	DGCCRF's financial needs will be adapted as seen fit for the implementation of the DSA. CNIL does not require additional resources at this point.	Arcom is currently composed of about 15 employees, of which 2/3 have knowledge about the DSA.	N/A

	DGCCRF's powers are broadened with the DSA in regard to: – Requesting a new type of civil injunction – Investigative powers (Art. 49(4) and 50(2) DSA) – Accessing online platforms service providers' data (Art. 40 DSA) CNIL's powers are broadened with the DSA in regard to: – Seizing any document under the judge's supervision – Recording interviewees"responses – Adopting corrective measures			
Germany	The BNetzA (DSC) can: – Conduct investigations by itself and ex officio (Art. 51 DSA) – Order the necessary measures to a provider who does not comply – Impose a monetary penalty (art. 52(1) and (4) DSA)	The estimated material costs are EUR 1.7 million	70 additional staff positions for the DSC are planned.	N/A
Greece	National Telecommunications and Posts Commission (DSC) can: – Impose fines and sanctions – Manage user complaints – Collect information from providers – Coordinate with other bodies – Cooperate with other Member States – Participate in the European – Digital Services Council with right to vote			

	– Recognize entities as "trusted flaggers" – Certify out-of-court dispute resolution bodies – Publish an annual report National Radio and Television Council can: – Supervise intermediate service providers (Art. 26(1) a, b, and c, 26(2), 28(1) DSA) – Participate in the European Digital Services Council without right to vote Personal Data Protection Authority can: – Supervise intermediate service providers (Art. 26(1) d, 26(3), and 28 DSA) – Participate in the European Digital Services Council without right to vote	The DSC's expenses are covered by fines, periodic monetary penalties, and supervisory fees (if applicable). The DSC may impose supervisory fees to service providers with establishment or legal representative in Greece.	The DSC has 217 employees. The National Radio and Television Council has 18 specialists and 17 permanent administrative employees. The Personal Data Protection Authority has 14 specialists and 50 administrative employees.	Fines and periodic monetary penalties shall be imposed only with a specially reasoned decision by the DSC or other authority and the service provider should have the chance to present its views.
Hungary	The NMHH's (DSC) can: – Impose fines for procedural infringements, including imposing fines on directors of a company – Adopt interim measures Impose fines on the subject of an investigation who fails to provide data or if the data is not satisfactory	N/A	The task has been allocated to the DG Online Platforms internally.	The implementing act provides for safeguards relating to the protection of secret information.

Italy	AGCOM's (DSC) competencies are broadened with the DSA in regard to: – Imposing sanctions	The budget for 2024 is EUR 4,005,457. The resources are financed from a supervisory fee of 0.135 per thousand of the turnover from the last approved balance sheet of intermediary service providers.	The AGCOM will have 23 additional employees.	N/A
Latvia	The DSC's investigative powers are: – Carrying out on-site inspections without authorization of the court – Requesting traffic data from an electronic communications undertaking The DSC's enforcement powers are: – Imposing penalties if a person interferes or resists the inspections	N/A	Six additional positions have been allocated to the DSC.	The control of the legality and administrative acts issued by the DSC will be ensured under Art. 7(5) of the State Administration Structure Law. It is also provided that the DSC shall be financed to the extent necessary to ensure the independence of its function and the effective application of the DSA.
Lithuania	The CRA's (DSC) competencies are broadened with the DSA in regard to: – Appointment of legal representatives of intermediaries – Certification of entities which may investigate disputes out-of-court – Assignment of trusted flaggers – Investigations of violations	The CRA's budget is EUR 120,000 for 2024–2026. There is no supervisory fee currently imposed.	The CRA's internal department dedicated to the DSA has 4 employees.	N/A

Netherlands	The ACM's (DSC) competencies are broadened with the DSA in regard to: – Certification of trusted flaggers – Certification of alternative dispute resolution entities and vetted researchers	N/A	The ACM will have 49 full-time additional employees. Currently, about 70 full-time employees are dedicated to the implementation of new digital legislation.	N/A
Norway	N/A	N/A	N/A	N/A
Poland	The draft proposal of December 2024 for implementing act for the DSA addresses the powers in the area of: – Certification of out-of-court dispute resolution bodies, vetted researchers, and trusted flaggers – Supervision of intermediary service providers (infringement proceedings, controls, imposing decisions/ restrictions) – Issuing orders (by DSC) addressing illegal content and unjustified restrictions imposed on service recipients Imposition of fines – User complaints	Draft proposal estimates cost limits for UKE as111 208 738 PLN in years 2025-2034 And for UOKiK 31 896 949,20 PLN for the same period	Draft proposal includes information about prospective new 30 employees for UKE and 11 for UOKiK	The decision to impose a fine should be subject to appeal to the Sąd Ochrony Konkurencji i Konsumentów.
Portugal	N/A	N/A	ANACOM (DSC) has 8 full-time employees dedicated to the DSA.	N/A
Romania	N/A	ANCOM (DSC) will apply supervisory fees from 2027.	ANCOM has a new department dedicated to the DSA, with currently 7 full-time employees and a goal of 21 employees in 2 years.	N/A

Slovakia	The DSC can: – Conduct an anonymised control purchase of the service or real-time recordings to document deficiencies in the service – Carry out on-site inspections and enter the premises without notice – Acquire, process, and evaluate information and documents provided by service providers – Impose appropriate interim measures or remedy measures	The DSC's budget is EUR 2,965,858 for 2024.	The DSC will have an increase of 49 employees in 2024–2026.	Procedural safeguards are guaranteed: – Right to refuse to disclose information if doing so create a risk of criminal prosecution – Right to refuse the audio-visual, video or sound recording – During the inspections, right of inviolability of home must be respected. – Inspected subject may be present at all individual acts of the inspection – A written confirmation on securing of copies of information provided must be provided. – Preliminary statement to a written record on the inspection procedure may be provided – A written record from the inspection must be provided – The procedure for issuing an interim measure and the decision on the objection is regulated by the Administrative Procedure Code
Slovenia	AKOS' (DSC) competencies are broadened with the DSA in regard to – Full inspection and prosecution powers – Certification of trusted flaggers	N/A	AKOS has a new internal unit, Digital Services Division, for the DSA.	N/A

	– Certification of out-of-court dispute resolution providers		This unit has currently 3 employees, with 2 additional employees foreseen by the end of 2024.	
Spain	CNMC's (DSC) investigative powers are: – Entering the premises of online service providers – Examining books – Make copies or extracts – Requiring access to be provided – Sealing premises – Asking for explanations – Asking questions New infringements are introduced: – Very serious infringements – Serious infringements – Minor infringements – Penalties of Art. 52 DSA are introduced. The CNMC has a new enforcement power: – Declaring commitments made by service providers binding or in the event of non-compliance, to continue with the sanctioning procedure		The DSC was planning on filling 7 vacancies.	The exercise of the investigative powers will require judicial authorisation where the right to inviolability of the home on premises other than those of the business is at issue.
Sweden	On top of the powers granted by the DSA, the Complementary Act provides supplementary provisions.	Estimated that approximately SEK 24 million per year would be needed.	N/A	Procedural safeguards are already in Swedish law (Instrument of Government, Administrative Procedure Act, Administrative Court Procedure Act).

Question 3. Initial experiences under the DSA

What are the initial experiences with national competent authorities acting under the DSA (if any)? Did the authorities undertake any scoping exercises to map which companies are being regulated by the DSA in the Member State? Did they announce any enforcement priorities?

Some DSCs have started providing guidance to companies to help them comply with the DSA, whether directly (e.g., by discussing with them) or indirectly (e.g., by publishing information on their website). Rapporteurs for Denmark and Portugal have said that these Member States have experience in receiving and screening complaints.

Eight Member States have conducted studies to map the companies regulated by the DSA in their territory.

	Initial experiences	Companies regulated by the DSA	Enforcement Priorities
Austria	N/A	A study is currently being conducted but has not been completed.	Initially, the priority was to handle the contact points (Art. 11 DSA).
Belgium	N/A	BIPT commissioned a study in 2024 and found that around 500 intermediary services fall under their jurisdiction.	Since BIPT is not fully staffed, it is prioritizing a risk-based approach, by contact services that present the highest risk to users.
Bulgaria	N/A	N/A	N/A
Croatia	N/A	N/A	N/A
Czechia	HAKOM (DSC) has exchanged contacts and participated in the working group to draft the implementing act.	Companies have to self-identify and notify the DSC. A scoping exercise was completed.	N/A
Denmark	The DSC has taken initiatives to implement the DSA: – Informed the identified companies about the DSA – Conducted the initial examination of all complaints received (which mainly concern platforms established in other Member States or in third countries)	A study to identify the companies was conducted, but it is not publicly available. The necessity for a scoping exercise will be assessed in 2025.	

	– Identified cases where the DSA is relevant and in serious cases, informed the victims of their options to complain. So far, the DSC's experience has been much more about screening the complaints and forwarding them to the Commission or Digital Services Coordinators and competent authorities in the relevant Member States.		
Finland	N/A	N/A	N/A
France	Arcom (DSC): It has started guiding companies to help them comply with the DSA. It is in contact with professional federations and legal networks which might help companies.	Arcom: It is up to the companies to self-identify. DGCCRF: It has identified about 20 marketplaces subject to the DSA. One of the difficulties is due to the fact that some entities are hybrids (physical stores and e-commerce platforms).	Arcom: Priorities are set by the European Digital Services Council. In June 2024, the priority was to protect the digital ecosystem in light of the elections. Currently, the priority is the protection of minors and of the youth online. DGCCRF: By the end of 2024, it will launch a national investigation with about 20 large entities to control their compliance with the DSA. CNIL: Priorities are not defined yet, but the protection of minors and online advertising have been highlighted.

Germany	N/A	A study and database have been created.	N/A
Greece	The DSC has taken initiatives to implement the DSA: – Creation of the Registry of Intermediary Service Providers including Host Services – Publication of the procedure for the certification of trusted flaggers	N/A	N/A
Hungary	Two studies on dark patterns have been commissioned to delimit enforcement powers under DSA and UCPD.	The DSC mapped and contacted domestic online platform providers to help them comply.	N/A
Italy	AGCOM (DSC) has taken initiatives to implement the DSA: – Initiated preliminary analysis to identify the procedure for filing a complaint (Art. 53 DSA) – Issued a notice concerning the modalities for communicating contact points (Art. 11 DSA) – Issued a notice concerning modalities for designating legal representatives (Art. 13 DSA) – Issued a notice concerning the modalities for communicating the number of active recipients (Art. 24(2) DSA) – Adopted a decision concerning the procedure to certify out-of-court dispute resolution bodies (Art. 21 DSA) – Adopted a decision concerning the procedure to certify trusted flaggers (Art. 22 DSA)	N/A	N/A

Latvia	N/A	Data is unclear, but it is estimated that there are at least 300 different intermediary service providers in 2024.	N/A
Lithuania	CRA (DSC) has set up an internal task force and has started publishing information to help users and entities understand the DSA on its website.	N/A	For 2024: – Preparatory activities (preparing implementing acts, procedures, and principles) – Adapting information systems
Netherlands	N/A	N/A	N/A
Norway	N/A	N/A	N/A
Poland	N/A	Reports have been done by national authorities, but not directly in the context of the DSA.	N/A
Portugal	ANACOM (DSC) has already received 12 complaints, which ranged from account blockages to the lack of communication channels with the platforms. It set up a team of 8 people to address the coordination task. However, it foresees that a team of 12 to 20 people will be needed. 4 requests to become trusted flaggers have been received.	ANACOM will launch a brief study to identify intermediary service providers in Portugal. So far, 100 providers have already been identified.	N/A
Romania	ANCOM (DSC) has undertaken extensive discussions with other national authorities for the enforcement of the DSA.	N/A	N/A
Slovakia	N/A	N/A	N/A

Slovenia	N/A	N/A	For 2025–2030: – Ensuring a transparent and secure online environment – Monitoring the situation in Slovenian and EU markets and identifying key challenges to respond promptly – Effective and rapid participation in supervisory procedures – Developing predictable and effective regulatory practices – Cooperating with other Member States
Spain	N/A	N/A	N/A
Sweden	N/A	N/A	N/A

Question 4. Allocation of DMA competences

What tasks are allocated to competition authorities for the DMA enforcement? Do the authorities have the competence and investigative powers to conduct investigations into possible non-compliance with the obligations laid down in the DMA (under Article 38(7) DMA) and if so, how is this set up?

Most of the Member States have reported tasks relating to assisting and supporting the European Commission ("Commission") for their competition authorities.

Only four Member States have answered that their competition authorities do not have investigative powers. France has noted that its competition authority's investigative powers were not amended with the DMA. As a result, it could only discover non-compliance with the DMA while investigating under different regulations. The Swedish competition authority can only investigate upon the Commission's request but cannot initiate investigations.

	Tasks of Competition Authorities	Investigative Powers
Austria[a)]	N/A	The Federal Competition Authority ("FCA") has investigative powers.
Belgium	The Belgian Competition Authority ("BCA")'s competencies: – Receive complaints from third parties – Inform the Commission in case of suspected non-compliance – Request the Commission to open a market investigation (Art. 41 DMA) – Receive information from the Commission on concentration of gatekeepers (Art. 14 DMA) – Refer concentrations to the Commission Communities Authorities are competent for audio-visual media services.	The BCA has the same investigative powers for the DMA as under national competition law.
Bulgaria[b)]	N/A	N/A
Croatia	The Croatian Competition Agency's ("CCA") competencies: – Coordinating and supporting the Commission – Notifying the Commission about its intention to open a proceeding against the gatekeeper – Informing the Commission about the implementation measures (sending a draft of the measures at the latest 30 days prior to their adoption) – Informing the Commission of the imposition of interim measures as soon as possible	The CCA does not conduct investigations only based on the DMA. It informs the Commission about the potential case against the gatekeeper by the implementation of competition rules. It can perform certain investigatory steps for the Commission.
Czechia	The Office for Protection of Competition's ("OPC") competencies: – Provide assistance and cooperation to the Commission – Seek assistance from the companies when necessary	No investigative powers specified in the law. Presumably, the OPC would need specific legislative authorization on DMA grounds.

[a)] Specific national regulations relating to the DMA are still outstanding.

[b)] There is no current national legislation allocating powers to national authorities for DMA matters.

Denmark	The competencies of the Danish Competition and Consumer Authority include: – Request the Commission to open a market investigation. – Have the right to access information, including algorithms and tests, as well as explanations regarding these elements, as deemed necessary to fulfill the Authority's responsibilities. – May conduct interviews with legal or natural persons, provided they are deemed to have relevant information.	The Danish Competition and Consumer Authority has investigative powers. It decides whether an investigation needs to continue or be suspended. It must inform the Commission before taking any investigative measure. It may inform the Commission of the findings after an investigation is completed, which the Danish Competition Council must approve before the conclusions of the investigation are sent to the Commission.
Finland	The Finnish Competition and Consumer Authority's competencies ("FCCA"): Have the right to access to information regarding gatekeeper companies and from third parties, and may forward this information to the Commission (Art. 21(5), 27, and 53(4) DMA) Assist the Commission in conducting inspections and market surveys (Art. 23 and 16(5) DMA) Request the Commision to open a market investigation. No new competencies were given to other national authorities than the FCCA.	No investigative powers based on Art. 38(7) DMA were given to national authorities because of the lack of gatekeepers in Finland.
France	N/A	Competition authorities have the same investigative powers under the DMA as they did prior to investigating mergers and anti-competitive practices. This means that authorities could discover a violation of the DMA while investigating under different regulations. The investigative powers: – Hearing of a natural or legal person on the premises of a company, with possible assistance from the competent national authority (Art. 22(2) DMA)

		Inspections requested by the Commission (Art. 23(3) DMA) – Requiring the company or association of companies to provide access to its organisation, operation, computer system, algorithms, data processing and commercial practices (Art. 23(4) DMA) – Active assistance to the Commission (Art. 23(7) and (10) DMA) – Investigation at the request of the Commission (38(6) DMA) – Investigation on its own initiative (38(7)
Germany	N/A	National competition authorities have investigative powers. The Federal Cartel Office can decide to open or not an investigation. It is obliged to inform the Commission of the findings of an investigation. It can publish reports on the findings. If they are published, the company concerned may have to be granted the right to be heard. In parallel to an investigation, administrative proceedings can be conducted. The investigative powers: – Gathering of necessary evidence – Seizing evidence – Requesting of information – Requesting of documents – Inspect and examine business documents during business hours – Search business premises, homes, land and property of companies These powers are limited to matters with a potential impact on Germany.

Greece	The Competition Commission is tasked with (Art. 38 and 39 DMA): – Cooperation with the Commission – Informing the Commission before any investigation or obligation is imposed – Supporting the Commission when required – Forwarding copies of any written judgment of national courts regarding the DMA to the Commission	The Competition Commission has investigative powers.
Hungary	The Enforcement Unit will assist in dawn raids. The Legal Assistance Unit will deal with court procedures. For all other matters, the General Vice-President will appoint an investigator. For enquiries from the Commission, the Cabinet of the President is competent. The Antitrust Unit is responsible for procedures under Art. 80/S Tpvt. For the meetings at the High-Level Group, the President appoints the representative after consulting and approval by the President of the Competition Council and the Unit Supporting Decision-making.	The GVH has investigative powers. Investigations should be concluded by an order of the investigator transmitting the report to the Commission.
Italy	The ICA is tasked with: – Coordination and cooperation The Data Protection Authority is tasked with: – Data protection – Confidentiality	The ICA has the same investigative powers under the DMA as it has under the national competition law. It can use the information collected from an investigation for more general purposes (e.g., to enforce agreements restricting competition, abuse of dominant position, abuse of economic dependence, and merger control). It must inform the Commission before initiating an investigation.

		It must have a resolution that is communicated to the gatekeepers and to those who have filed complaints or petitions related to the investigation. The investigative powers: – Request information – Hold hearings – Conduct inspections Participating parties in an investigation may submit pleadings and have the right to access documents, the disclosure of which must not hinder the Commission's investigation or the adoption of implementing acts.
Latvia	The competition authority is tasked with: – Providing support to the Commission – Providing necessary assistance to the Commission in the preparation and execution of Art. 23 DMA	The competition authority has investigative powers: – Request information – Take statements – Carry out announced or unannounced visits to business premises – Conduct dawn raids warranted by the court
Lithuania	N/A	The authorities do not have investigative powers.
Netherlands[c)]	N/A	The ACM has investigative powers based on the DMA and based on previous existing powers. However, the ACM cannot investigate private homes for DMA matters, while it can under national competition law.
Norway[d)]	N/A	N/A
Poland[e)]	Prezes UOKik is tasked with: – Being a member of the High Level Group (Art. 40 DMA) – Assist the Commission to conduct interviews and take statements (Art. 22(2) DMA) – Assist the Commission when conducting inspections (Art. 23(7) to (9) DMA)	Prezes UOKik has investigative powers. Investigative powers: – Decide to conduct an investigation or not – Collect evidence in the course of the investigation

[c)] The DMA Implementation Act is currently pending before the House of Representatives.
[d)] The DMA is not yet applicable in Norway.
[e)] The act implementing the DSA has not been adopted yet.

	– Receive information regarding DMA violation (Art. 27 DMA) – Cooperate with the Commission (Art. 38(1) to (6) DMA)	– Authorize an employee of Urząd Ochrony Konkurencji i Konsumentów ("UOKIK") to take statements during an investigation led by the Commission (Art. 22 DMA) and to assist the Commission (Art. 22 DMA) – In cases where gatekeepers object to an investigation, employees of UOKIK can enter office premises, request access to documents, request explanations, secure evidence or seek assistance from the police or other organizations
Portugal[f]	N/A	N/A
Romania	N/A	The Romanian Competition Council ("RCC") has investigative powers. The RCC has to inform the Commission before starting any investigation. The RCC has to submit the findings to the Commission.
Slovakia	N/A	The Antimonopoly Office of the Slovak Republic has investigative powers. Investigative powers: – Investigate to determine if there is a basis for a request for a market investigation (Art. 41 DMA) – Require from any person any information or documents necessary – Make copies and extracts, or require official translations of these documents – Require oral explanations – Investigate on all premises and means of transport which are related to the activity of the company – Seal documents or media on which information is recorded – Seal premises, equipment, or means of transport – To secure access to information stored on an electronic form

[f] No specific measure to regulate the domestic application of the DMA has been adopted yet.

Slovenia	The Slovenian Competition Protection Agency ("AVK") is tasked with: – Cooperation and coordination with the Commission	Slovenia amended its Prevention of the Restriction of Competition Act (ZPOmK-2) to regulate the procedure and competence for enforcing the DMA and granting the powers to the AVK. The AVK has investigative powers under national competition law.
Spain	The Comisión Nacional de los Mercados y la Competencia (CNMC) is tasked with: – Receiving complaints (Art. 27 DMA) – Deciding on the appropriate measures to take to enquire about a complaint – Informing the Commission before taking investigative measures (Art. 38(7) DMA)	The CNMC has investigative powers. Investigative powers: – Conducting interviews and inspections – Recording and elaborating a transcript of the interviews – Requiring the presence of particular members of the staff when conducting a raid and asking them for particular documents – Powers contained in art. 23(2) DMA – Requesting the corresponding judicial authorisation – Investigating information confidentially without notifying the proceedings to the undertakings – All natural or legal persons and bodies of public administration must collaborate with the CNMC – The information collected during DMA-related investigations may also be used for other competition-related cases
Sweden	N/A	The Swedish Competition Authority does not have investigative powers to initiate and conduct its own investigations under Art. 38(7) DMA. It can conduct investigations at the Commission's request and can support it.

Question 5. Special rules for DMA

Which specific rules, resources or other measures have been adopted regarding the supervisory, investigative and enforcement powers of the competent authorities under the DMA? (e.g., allocation of powers and resources, procedural safeguards, supervisory fees, etc.) How many staff are dedicated to the DMA enforcement?

Regarding staff resources, competition authorities have or will have between one to sixteen employees dedicated to the DMA. Many have noted that no additional resources would be allocated to their competition authorities.

Of three Member States who provided an answer to the financial resources aspect, two said that no additional resources would be allocated.

	Financial Resources	Staff Resources	Procedural Safeguards
Austria	N/A	N/A	N/A
Belgium	N/A	The BCA has 6 full-time employees for the DMA.	N/A
Bulgaria	N/A	N/A	N/A
Croatia	N/A	The CCA has a separate digital unit, which will have 1 employee whose sole responsibility is DMA enforcement.	N/A
Czechia	N/A	N/A	N/A
Denmark	The yearly budget is EUR 536,303.	The Competition and Consumer Authority will have 1 full-time employee dedicated to the DMA.	N/A
Finland	N/A	N/A	N/A
France	No additional resource allocated. A tax could be implemented, but it has yet to be evaluated first.	No additional resource allocated.	N/A
Germany	N/A	Two Decision Divisions within the Federal Cartel Office are dedicated to the digital sector.	N/A
Greece	N/A	N/A	N/A
Hungary	N/A	No specific unit dedicated to the DMA.	N/A
Italy	No additional resource allocated.	No additional resource allocated. The ICA underwent reorganization and has now a Digital Platforms and Communications Directorate.	N/A

Latvia	EUR 154,631.00 for 2024. EUR 151,521.00 for 2025. EUR151,621.00 for subsequent years.	Two new staff positions will be added.	N/A
Lithuania	N/A	N/A	N/A
Netherlands	N/A	The ACM will receive 7 additional full-time employees. Cross-use of resources with other authorities is possible.	Officials must carry an identification card. Officials can only exercise their powers insofar as it is necessary for the performance of their duties. Private homes can only be entered with a prior judicial authorization and the official must write a report on the entry.
Norway	N/A	N/A	N/A
Poland	N/A	N/A	N/A
Portugal	N/A	N/A	N/A
Romania	N/A	The Competition Council has two new departments dedicated to the DMA, with 4 employees. No additional resources allocated.	Procedural guarantees are offered by the Commission as the sole enforcer of the DMA,
Slovakia	N/A	N/A	N/A
Slovenia	N/A	N/A	N/A
Spain	N/A	N/A	N/A
Sweden	N/A	A unit of 16 agents is tasked with responsibility for the DMA.	N/A

Question 6. Initial experiences under the DMA

What are the initial experiences with national competent authorities acting under the DMA (if any)? Did the authorities announce any enforcement priorities?

A few Member States reported that their competition authorities have consulted with the Commission and/or other groups such as the Advisory Committee and the High Level Group. Belgium stated that its competition authority held

consultations with gatekeepers. Spain has reported two cases related to the DMA involving Booking.com and Apple.

Of five Member States who provided an answer concerning enforcement priorities, three have mentioned international cooperation as a priority.

	Initial experiences	Enforcement Priorities
Austria	The Federal Competition Authority is primarily contributing its experience from competition enforcement to the High-Level Group and the Advisory Committee.	N/A
Belgium	The BCA held consultations with gatekeepers and small business users, but no case has been opened. A short guide was published for business users.	N/A
Bulgaria	N/A	N/A
Croatia	No relevant experience so far, and a low level of activities is expected given Croatia's small market. The CCA has conducted market research for food delivery services and online accommodation reservation services.	For 2024, the CCA did not address the DMA directly, but has set as a priority the investigation of exclusionary conduct by dominant companies.
Czechia	N/A	N/A
Denmark	The Authority expects the tasks to be largely coordinated with the Commission.	N/A
Finland	N/A	N/A
France	N/A	The priority is to establish the boundary between the DMA and abuses of a dominant position, prohibited by Art. 102 of the TFEU to decide whether prohibited practices under Art. 102 TFEU fall under the DMA.
Germany	N/A	N/A
Greece	N/A	N/A
Hungary	N/A	N/A
Italy	The ICA has been cooperating closely with the Commission: Digital Market Advisory Committee (Art. 50 DMA) High Level Group (Art. 40 DMA) European Competition Network Informal exchanges	N/A

Latvia	The competition authority participated in the High-Level Group and the Advisory Committee.	For 2024: Monitoring of rapidly evolving and innovative markets Active cooperation with Member States, the OECD, and the Commission
Lithuania	N/A	N/A
Netherlands	N/A	N/A
Norway	N/A	N/A
Poland	N/A	N/A
Portugal		For 2024: Monitoring of trends and developments in the digital area to map out appropriate solutions Strengthening of international cooperation
Romania	N/A	N/A
Slovakia	N/A	N/A
Slovenia	The AVK has cooperated with: The Commission The Advisory Committee The European Competition Network.	N/A
Spain	The CNMC was involved in 2 cases: Booking.com, but which only became a designated gatekeeper after the proceedings Apple regarding the potential unfair terms it had imposed on app developers using the App store	Priorities include: Digital markets Cooperation with the Commission and the European Competition Network
Sweden	Informational efforts to enhance awareness surrounding the DMA: Updating the website Dissemination of information to the public through various channels The competition authority has received inquiries and complaints from business organisations. The competition authority received a tip concerning a gatekeeper, which was reviewed and forwarded to the Commission.	N/A

Section 2: Use of National Legislative Leeway Under the DMA/DSA

Question 1. Pre-emption by the DSA

How are the MSs dealing with the pre-emption effects of the DSA? What happened to the (partially) overlapping pre-existing national laws? (e.g., hate speech notification laws, implementations of the E-Commerce Directive, including provisions on search engines, etc.)

Of the twenty-three Member States, fifteen have answered that provisions in the national laws implementing the E-Commerce Directive have been repealed or will be. Among others, laws concerning consumer protection and cyber-security as well as civil and criminal codes have been partially repealed for overlapping with the DSA. Greece reported that since the national laws and the DSA apply cumulatively, no amendments have been made. Poland noted that the current lack of provisions on search engines creates a legal gap.

	Amendments made to national laws
Austria	Austria refrained from repealing regulations applicable to intermediary services in conformity with Union law, e.g., Hate Online Combating Act. Some sections of the E-Commerce Act were repealed: – s. 13-17 now Art. 4-6 DSA – s. 18 now Art. 8 DSA regarding the monitoring obligation of service providers and (new) S. 13 E-Commerce Act regarding the right to information – s. 19(1) now Art. 4(3), 5(2), 6(4) DSA The Austrian Communications Platforms Act was repealed entirely.
Belgium	Sections of the Economic Law Code were repealed: – Liability of intermediaries – Non-general monitoring obligation of intermediaries – Injunctions and duties to inform competent authorities and law enforcement authorities of illegal activities
Bulgaria	The approach of the draft bill is to make references to powers under the DSA but without abrogating the local legislation.
Croatia	Electronic Media Act: – No overlap, because it does not regulate the behaviour of service providers directly E-Commerce Act: – Overlaps with Art. 4,5, and 6 DMA, but the draft implementing act would repeal them Currently, there is an intention to implement new sectoral regulation that would overlap with the DSA.

Czechia	No modifications have been made yet, but the implement act proposal has been put forward to update existing regulations. The proposal focuses more on procedural obligations, e.g., penalties, since the DSA imposes substantive obligations. The proposal would amend: – Act on Some Information Society Services – Act on On-Demand Audiovisual Media Services – Cybersecurity Act – Act on Consumer Protection – Civil Code There does not seem to be an intention to adopt specific rules at the national level.
Denmark	Section 14-16 of the E-Commerce law were repealed.
Finland	Sections of the Act on Provision of Electronic Communications Services were repealed: Chapter 22: conditional exemption from intermediary liability
France	The Law on confidence of digital economy is amended: – Many definitions refer to Art. 2 DSA – Intervention of judicial authority is adapted – Sections relating to the DSC are created – Sections relating to the anticipation of the DSA are removed Consumer Code is amended: – Definition of "platform" refers to Art. 2 DSA. – DGCCRF is designated as an authority along with Arcom and CNIL The Law on freedom of communication is amended relating to the Arcom's powers. The Law on combating the manipulation of information is amended. The Law on Data Processing, Data Files and Individual Liberties is amended to designate the CNIL as an authority.
Germany	The Network Enforcement Act was almost completely repealed. The Telemedia Act was completely repealed. The Interstate Media Treaty was amended: – Sections on the responsibilities of the state media authorities
Greece	The DSA and the existing legislation cumulatively apply.
Hungary	The implementing act complements the DSA and amended other laws, such as copyright, media law, and electronic commerce rules.
Italy	N/A

Latvia	Amendments to Cabinet of Ministers 08.02.2022 Regulation No. 99 are required. The Ministry of Economics is currently assessing if it is necessary to adopt a new regulation to replace Regulation No. 99.
Lithuania	The Law on Information of Society Services was amended: – Sections on the liability of intermediaries were removed – Sections implementing the E-Commerce Directive were removed – Section on the liability of mere conduit, caching, and hosting service providers was added (Art. 4-6 DSA) Legislation on notice and take down mechanism was repealed.
Netherlands	Dutch Civil Code will be amended: – Section on the liability exemption for providers of mere conduit, caching, and hosting services will be removed Dutch Code of Criminal Procedure will be amended: – Sections on the confidentiality of orders and claims addressed to providers and the postponement of notification to a recipient of a service will be amended
Norway	N/A
Poland	A proposed amendment of the Act on Providing the Services Electronically is the removal of the liability exemptions for providers. There are no specific provisions for search engines, which creates a legal gap. The legal doctrine proposes that the liability exemption for search engines should be clearly addressed in the future amendments. There is a potential conflict between the powers of Prezes KRRiT to order disabling access to certain content and impose penalties to video-sharing platforms, and the powers of the DSC.
Portugal	Proposed amendments are not made public. The current overlaps relate to: – Liability of intermediary service providers. – Supervising, monitoring, removing, and preventing access to protected content (Art. 9 DSA) – Joint liability between online marketplace providers and sellers – Portuguese Charter on Human Rights in the Digital Age (no direct overlap)
Romania	Some sections of the law implementing E-Commerce Directive were repealed.
Slovakia	Sections that overlapped with the DSA were repealed: – Act No 22/2004 Col. Art 6 - Exclusion of liability of the service provider (Arts. 4-6, 8 DSA) was repealed. The Act on electronic commerce was repealed relating to the liability exemption of service providers.
Slovenia	The Electronic Commerce Market Act was repealed relating to the liability of intermediary service providers, data transmission, caching, and hosting services (Art. 4-8 DSA).
Spain	The implementing act has not been adopted.

Sweden	S. 4 of the BBS Act was amended because it overlapped with Art. 8 DSA regarding the imposition of a duty of oversight on providers. Sections of the E-Commerce Act that implemented Art. 12-15 of the E-Commerce Directive were amended because of the DSA.

Question 2. National rules on illegality

Did the Member States try to map the national rules on the illegality of content that is relevant for the DSA enforcement? Were there any notable DSA-related changes in such content rules recently?

Among the seven Member States who have conducted a mapping exercise, three have reported that their implementing acts contain some rules mentioning also the types of illegal content. Croatia's definition of illegal content contained in its implementing act is assumed to be exhaustive. Only France and Latvia have reported that their national regulations have been amended by the DSA concerning illegality of content.

	Mapping	Changes in content rules
Austria	The implementing act contains a list of regulations that is relevant for assessing illegal content. Illegal content is a violation of: – Civil law – Copyright law – Administrative law – Consumer protection or product safety law – Criminal law KommAustria has the "typologies of illegal content" on its website.	N/A
Belgium	N/A	N/A
Bulgaria	N/A	N/A
Croatia	The implementing act contains a definition of illegal content: – Criminal act or misdemeanour – Breach of personal data processing legislation – Breach of intellectual property rights – Breach of regulations within the State's – Inspector's powers (e.g., consumer protection and tourism)	No changes.

	– Violation of health, medicine, medical products, and biomedicine aspects It is implied that this list is exhaustive.	
Czechia	No mapping.	N/A
Denmark	A law regulating illegal content on social media was proposed, but it was withdrawn because of the imminent adoption of the DSA.	N/A
Finland	Legislation that deals with illegal content: – Act on Interference in the Dissemination of Terrorist Content Online – Act on Combating the Dissemination of Child Pornography – Copyright Act	N/A
France	There was mapping in the implementing act.	The implementing act modifies the following regulations on the illegality of content: – Law on confidence of digital economy – Consumer Code – Law on the freedom of communication – Electoral Code – Law on combating the manipulation of information – Data Processing, Data Files and Individual Liberties – Law on the status of newspaper and periodical grouping and distribution companies – Law aimed at preserving the ethics of sport, strengthening the regulation and transparency of professional sport and improving the competitiveness of clubs – Intellectual Property Code
Germany	No mapping.	No changes.
Greece	N/A	No changes.
Hungary	Rules identified in the Act CVIII of 2001: – An amendment to the liability rules for electronic commerce service providers – Intermediary service providers are obliged to remove infringing content if they become aware of its infringing nature – Provisions on complaints concerning infringements	N/A

Italy	No mapping.	No changes.
Latvia	N/A	National regulations have been amended to be compliant with the DSA, e.g., the Law on Information Society Services.
Lithuania	The only mapping is with the Law on Electronic Communications, which contains a list of competent authorities able to issue take down orders.	N/A
Netherlands	No mapping.	N/A
Norway	N/A	N/A
Poland	No mapping by the relevant authorities yet. Illegal content should be considered as violating: – Criminal law – Civil law – Intellectual property law – Consumer protection law – Competition law – Media law Rules identified: – Notification of illegal content – Role of NASK, a contact point for illegal content – Website blocking as a measure to address illegal content	No changes.
Portugal	No mapping. The Regulatory Entity for Social Communication stated that it should be made clear which authority will be responsible for illegal content.	No changes.
Romania	No mapping. The principle "what is illegal offline is illegal online" applies, so it has not been deemed necessary to define illegal content under the DSA.	N/A
Slovakia	No mapping.	No changes.
Slovenia	No mapping.	No changes.
Spain	No mapping.	No changes.
Sweden	There was mapping.	No further changes than those mentioned in Question 1.

Question 3. Implementation of the DSA

Apart from the institutional implementation of the DSA, what other related legislative acts were/are considered or adopted on the national level? (e.g., laws on influencers or other content creators, content rules, etc.)

Seven Member States have reported that DSA-related laws have been modified, will be adopted, or are currently under discussion to be adopted. France, Italy, Poland, and Romania have mentioned in this context a law for the protection of minors. France has reported that its law on influencers was modified because of the DSA and Romania is currently issuing recommendations to influencers. Besides that, laws on online violence, freedom of press and deep fakes are being discussed for adoption.

	Other relevant laws
Austria	Already in place before the DSA: – The E-Commerce Act to strengthen the legal position of the victim and law enforcement of online hate
Belgium	No other laws are being considered except those already in place.
Bulgaria	The bill envisions that respective authorities should issue instructions (form of subordinate legislative instruments) for coordination of exercise of their powers.
Croatia	No other laws are being considered except those already in place.
Czechia	No other laws are being considered except those already in place.
Denmark	Already in place before the DSA: – The marketing law to protect children – Government has an expert committee to examine and recommend actions to big search engines, platforms, and social media
Finland	N/A
France	Modified by the DSA: – The Act on the regulation of commercial influence – The Act introducing a digital majority – Titles I and II of the Security and Regulation of Digital Space Act on the protection of minors against pornography and child pornography
Germany	Will be adopted: – A law against digital violence
Greece	Already in place before the DSA: – Legislation about e-commerce and consumer protection – Legislation about hate speech – Legislation about data protection – Legislation about equal treatment in service provision

Hungary	Amendment of Act LXXVI of 1999 on Copyright Amendment of Act CLXXXV of 2010 on Media Services and Mass Media Amendment of Act XXIII of 2023 on cybersecurity certification and cybersecurity supervision Amendment of Act CXCIV of 2011 on the Economic Stability of Hungary Amendment of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services
Italy	Modified by the DSA: – Law implementing the Directive on Audio-Visual Services to limit communication of audio-visual content by a provider from another Member State – Decreto Caivano for the protection of minors Already in place before the DSA: – Decreto Caivano for the protection of copyright Adopted after the DSA: – (Not legislative) Guidelines on influencers as some obligations imposed on influencers are parallels to the DSA
Latvia	No other laws are being considered except those already in place.
Lithuania	Already in place before the DSA: – Guidelines on Marking information in Social media
Netherlands	No other laws are being considered except those already in place. Already in place before the DSA: – Social Media & Influencer Marketing Advertising Code – Child and Youth Advertising Code – Code of Conduct on Transparency of Online Political Advertisements
Norway	Discussions are currently being held about the need to adopt complementary legislation, e.g., protection of press freedom on digital platforms.
Poland	New: government proposal for law protecting minors from harmful content online; planned for 2025.[a)] Already in place before the DSA: – Law combatting the unfair competition and the unfair market practices – The proposal on the freedom of speech in the social media (2021) might be in conflict with the DSA (dropped)
Portugal	No other laws are being considered except those already in place. Already in place before the DSA: – Law on monitoring, controlling, removing, and preventing access in the digital environment to content protected by copyright and related rights – Influencer Marketing – Information on Rules and Good Practices in Commercial Communication in the Digital Media (Guidelines)
Romania	– Proposals for protection of minors – Proposals for measures against deep-fake content – Recommendations issued to influencers on disclosing commercial intent

[a)] https://www.gov.pl/web/premier/projekt-ustawy-o-ochronie-maloletnich-przed-dostepem-do-tresci-szkodliwych-w-internecie

Slovakia	Already in place before the DSA: – Consumer protection laws – Media Services Act
Slovenia	No other laws are being considered except those already in place. – Draft of the Mass Media Act for the regulation of online safety and influencers
Spain	No other laws are being considered except those already in place. Already in place before the DSA: – Law on Information Society Services and Electronic Commerce – General Law on Audiovisual Communication – General Law on Advertising – Law on Unfair Competition
Sweden	No other laws are being considered except those already in place.

Question 4. Pre-emption by the DMA

How are the MSs dealing with the pre-emption effects of the DMA? (e.g., other rules ensuring fairness and contestability in digital markets)

Most Member States have reported that there was no overlap between the DMA and the national legislation. Only Latvia, Slovenia and Slovakia mentioned provisions of their competition laws were amended. Italy and Spain stated that there might be overlap between the DMA and their national laws on the abuse of economic dependence.

	Dealing with pre-emption effects
Austria	No overlap with national legislation. It coexists with competition law.
Belgium	Two sections of the Economic Law Code might interact with the DMA (but no overlap): – Section on competition law that prohibits the abuse of economic dependency which applies to gatekeepers designated by the DMA – Section on market practices to ensure B2B fairness
Bulgaria[a)]	N/A
Croatia	No overlap with national legislation, because there are no laws to ensure fairness and contestability in digital markets. The only effect is that the DMA prohibits the CCA from conducting investigations under Art. 101 and 102 TFEU, which is in the implementing law.
Czechia	No overlap with national legislation. It coexists with competition law.
Denmark	No overlap with national legislation. It coexists with competition law and electronic commerce law.

[a)] No national legislation implementing the DMA yet.

Finland	N/A
France	Supposedly, no overlap with national B2B law. There could theoretically be overlap with competition law.
Germany	No overlap with national legislation. It coexists with competition law.
Greece	No overlap with national legislation.
Hungary	The rules are applied directly.
Italy	There might be overlap between the DMA and the national law on the abuse of economic dependence.
Latvia	The Competition Law of the Republic of Latvia has been amended: – Investigative powers – Assistance to the Commission – Damages Current amendments are under discussion relating to expanding the competition authority's powers to monitor the abuse of economic dependence.
Lithuania	No overlap with national legislation.
Netherlands	No overlap with national legislation.
Norway	It is unlikely that there will be overlap with competition law.
Poland	No overlap with national legislation. It coexists with competition law.
Portugal	N/A
Romania	No overlap with national legislation. It coexists with competition law.
Slovakia	Sections of national laws that conflicted with the DMA were repealed.
Slovenia	The national competition law was amended to be aligned with the DMA.
Spain	A potential overlap is Art. 3 of the national Competition Act, which prohibits abuse of economic dependence.
Sweden	No pre-emption effects identified yet.

Question 5. Implementation of the DMA

Apart from the institutional implementation of the DMA, what other related legislative acts were/are considered or adopted on the national level?

Only a few Member States are considering adopting new legislation. Austria has reported that many whistleblower-related acts were modified by the DMA. In Finland, the Netherlands, and Norway, there is discussion for the adoption of complementary legislation concerning namely, investigative powers.

	Other relevant laws
Austria	Already in place before the DMA: – Federal Whistleblower Protection Act – State laws regulating whistleblowing protection Modified by the DMA: – Upper Austrian Whistleblower Protection Act – Carinthian Provencal Code of Law – Carinthian Whistleblower Protection Act – MiCA Regulation Enforcement Act – Lower Austrian Information Act – Lower Austrian Whistleblower Protection Act
Belgium	No other laws are being considered except those already in place.
Bulgaria	N/A
Croatia	No other laws are being considered except those already in place.
Czechia	No other laws are being considered except those already in place.
Denmark	No other laws are being considered except those already in place.
Finland	There is a need for complementary provisions concerning: – Information exchange between national authorities and the Commission (Art. 21, 27, 38, and 53 DMA) – Requests and assistance in market investigations (Art. 16(5) and 41 DMA) – Investigative and enforcement powers (e.g., Art. 23(8) DMA)
France	No other laws are being considered except those already in place.
Germany	No other laws are being considered except those already in place.
Greece	Already in place before the DMA: – Legislation about competition – Legislation about e-commerce – Legislation about unfair commercial practices – Legislation about the provision of services
Hungary	No other laws are being considered except those already in place.
Italy	N/A
Latvia	Already in place before the DMA: – Civil Procedure Law
Lithuania	No other laws are being considered except those already in place.
Netherlands	No other laws are being considered except those already in place. However, there is discussion about the introduction of 2 new competencies for the competent authority: – Investigation tool – Call-in power
Norway	There is discussion about the need for additional legislation outside of the DMA.

Poland	No other laws are being considered except those already in place.
Portugal	N/A
Romania	N/A
Slovakia	N/A
Slovenia	No other laws are being considered except those already in place.
Spain	An amendment was introduced to Art. 18 of the Competition Act.
Sweden	No other laws are being considered except those already in place.

Section 3: Vertical and Horizontal Public Enforcement-Related Cooperation Under the DSA/DMA

Question 1. Procedural rules for the DSA/DMA

What procedural or other rules related to the DSA and DMA are relied upon to create effective cooperation, both between national competent authorities of various Member States among themselves and with the European Commission? Do you see any potential challenges in this regard?

In regard to the DSA, half of the Member States reported that their implementing acts set out rules for cooperation between authorities, while others did not implement specific rules beyond what the DSA requires. Among the challenges highlighted, Austria and Portugal have pointed out the difficulty in maintaining the independence of the DSC vis-à-vis the Commission. Moreover, Austria and Lithuania mentioned the challenge of responsibilities overlapping between national authorities as well as with the Commission.

In regard to the DMA, only Belgium and Hungary implemented specific rules concerning cooperation between national authorities. Among the challenges highlighted, Austria, Finland, and Germany stated that the interactions between national competition law and EU law might give rise to difficulties. Belgium and Portugal mentioned that the delineation of responsibilities between national authorities might pose a challenge.

	DSA	DMA
Austria	No specific rules in the implementing act but national law sets out: – Obligation to cooperate with Member States – Authorization to use results of foreign proceedings – Right to be heard – Right to access files and confidentiality restrictions Challenges: – Maintaining independence of the DSC vis-à-vis the Commission – Clear handling of responsibilities between the national authorities and the Commission – Ensuring equivalent and effective legal protection – Use of soft law acts	Challenges: – Challenge in enforcing the DMA due to the interfaces with competition law
Belgium	Cooperation Agreement sets out: – National information sharing system – Obligation for regulators to meet every 3 months – Questions of competences among regulators should be settled by consensus and by inter-ministerial committee if consensus is not possible – Regulators should check before issuing a sanction that an identical one has not already been issued by another regulator – Participation of the DSC and other regulators in the European Board for Digital Services The DSC is currently entering into bilateral agreements with federal regulators that are not competent under the DSA, e.g., Data Protection Authority.	Challenges: – 3 Communities authorities are expected to cooperate with the Commission (on top of the Belgian Competition Authority), but the imprecise nature of their powers, the lack of harmonization between their powers, and the lack of clear framework for cooperation with the Belgian Competition Authority Economic Law Code sets out: – Regulators can inform the Prosecutor General when they believe a market investigation is ecessary – The Prosecutor General should seek the opinion of other regulators – The Belgian Competition Authority Chairman may invite sectoral regulators to the Digital Markets Advisory Committee No specific rules beyond the DMA requirements regarding cooperation with the Commission.
Bulgaria	No national legislation that implements procedures.	No national legislation that implements procedures.

Croatia	Implementing act sets out: – Duty of cooperation between national authorities – DSC is required to ask for the opinion of the relevant authority when creating ordinances for out-of-court dispute resolution bodies and trusted flaggers. No specific rules beyond the DSA requirements regarding cooperation with other Member States and the Commission.	No specific rules beyond the DMA requirements.
Czechia	No specific rules beyond the DSA requirements.	No specific rules beyond the DMA requirements.
Denmark	Implementing act sets out: – The law applies irrespective of whether the inspection is carried out for the purpose of a national case or to assist Member States or the Commission	No specific rules beyond the DMA requirements.
Finland	Implementing act sets out: – Exchange of information and documents between authorities – Authorities can get information from criminal investigations – DSC can get information when necessary for suspected criminal offences (Art. 18 DSA) Challenge: – Delay for Member States to designate their DSC	No specific rules beyond the DMA requirements. Challenges: – Complexity of interplay between EU and national levels
France	Implementing act sets out: – National coordination network for digital services regulation including all the competent administrative authorities and State services Tripartite agreement between the competent authorities under the DSA (Arcom, DGCCRF, and CNIL) regulates their cooperation.	CNIL is part of the European Data Protection Board, which includes the Commission and other Member States.
Germany	Implementing act sets out: – In case of conflict with another Member State, the issue must be brought to the attention of the Commission without delay	The European Competition Network is the coordination mechanism with the Commission. No specific rules beyond the DMA requirements for cooperation between national authorities.

		Challenges: – It will be challenging to ensure a consistent enforcement practice of antitrust rules between national authorities in areas not covered by a DMA decision adopted by the Commission – Although there is an obligation to notify the Commission before imposing obligations on a gatekeeper, the national authority is not obliged to consult with or await an opinion from the Commission, so it remains to be seen to what extent the Commission can influence national authorities that may deviate from its assessment.
Greece	No rules regulate cooperation with other authorities, other Member States, and the Commission.	No rules regulate cooperation with other authorities, other Member States, and the Commission.
Hungary	The implementing act sets out that: – The President of the DSC shall cooperate with DSCs from other Member States, the Commission, and the European Digital Services Board – The President is entitled to request information from other DSCs and the Commission – The President shall provide the information at the request of other DSCs or the Commission. – The DSC shall cooperate with the competition authority – The President can, in a reasoned request, require the transfer of data submitted to another Member State's DSC if the data is necessary for the performance of the President's tasks.	A new chapter has been added to the Hungarian Competition Act regarding cooperation between the competition authority and the Commission: – When the Commission requests the GVH to open an investigation, the rules of the competition procedure apply with derogations specific for DMA investigations – If requested by the Commission or a competent authority under the DMA or by the DMA itself, the GVH shall make the information available – The GVH shall transmit a report to the Commission when investigating compliance with the DMA The Competition Act provides limitation to access to files: – The right of access to the file may not be disclosed where the absence of such documents or information would prevent the exercise of the client's statutory rights

Italy	The DSC signed a collaboration agreement with the Commission to define the procedural framework to exchange information, data, methodologies, systems, and tools to help identify systemic risks with VLOPs and VLOSEs. The DSC has also attended meetings with the European Board for Digital Services for coordination with other Member States.	N/A
Latvia	Implementing act sets out: – Competent authorities shall provide the DSC at its request an opinion within a month	State Administration Structure Law provides that: – Upon request, institutions are required to provide the necessary information or assistance, regardless of their hierarchical status The Competition Law provides that: – The competition authority shall provide all necessary support to the Commission in preparing and executing the activities of Art. 23 DMA – The national police force must assist the Commission where a market participant fails to comply with the procedural obligations of Art. 23(2) DMA – The competition authority is obligation to undertake procedural actions at the request of the Commission in cases involving potential violations of the DMA
Lithuania	Implementing act sets out: – Centralisation of information on take down orders – Distribution of complaints between competent authorities Challenges: – These rules assume that only one authority is competent and do not foresee potential overlap or cooperation between national authorities	N/A

Netherlands	No specific rules beyond the DSA requirements. The DSC had requested a rule according to which the orders to act against illegal content or to provide information sent by the national authorities should be shared with all authorities to avoid individual arrangements, but the request was denied.	No specific rules beyond the DMA requirements for cooperation with the Commission.
Norway	N/A	To be decided.
Poland	To be decided.	There are discussions to amend the Act on Protection of Competition and Consumers to ensure close cooperation between Prezes UOKiK and the Commission.
Portugal	ANACOM (the DSC)'s Statutes sets out: – ANACOM shall establish forms of cooperation at the national or European Union level when necessary or convenient – ANACOM shall ensure its representation at national and international bodies and forums Challenges: – The independence requirements can raise issues since they surpass the limited universe of current independent administrative bodies	Procedural rules set out by the DMA: – Formal consultation mechanisms between national authorities and the Commission – Coordinated investigation – Join enforcement of actions Challenges: – The separation of powers among the competent authorities might not be clear – Limited resources of national authorities – Complexity of transactional investigations involving multiple Member States
Romania	Implementing act sets out: – The DSC and national authorities can share data and consult each other – The DSC can request the support of any national authority – The DSC can request that national authorities participate in working groups	No specific rules beyond the DMA requirements for cooperation with the Commission. No challenges are foreseen.
Slovakia	Media Services Act sets out: – DSC prepares COM annual reports – DSC cooperates with the COM – DSC cooperates with other Member States and the Commission No major challenges expected.	Challenges are currently being observed.

Slovenia	No rules for cooperation with other Member States and the Commission. No major challenges so far, but they are to be expected.	No specific rules beyond the DMA requirements for cooperation with the Commission. As cooperation with the Commission and other national authorities is well established under Art. 101 and 102 TFEU, no additional challenges are foreseen.
Spain	N/A	No specific rules beyond the DMA requirements for other national authorities and Member States. For the Commission, a joint investigation unit has been created.
Sweden	The Complementary Act sets out: – The DSC is tasked with leading a coordination mechanism with relevant competent authorities – Competent authorities must provide the DSC with information and support	N/A

Question 2. Interaction with national courts

Which measures apply specifically to the role of national courts and their interaction with the European Commission (COM) in the context of the DSA and DMA (e.g., possible submission by COM of written or oral observations, avoidance of national court decisions running counter to COM decisions, transmission of national judgments)?

Most of the Member States have not implemented specific measures, so interactions with the Commission would rely on Article 82 of the DSA and Article 39 of the DMA. The Netherlands amended their General Civil Procedural Code to allow civil courts to judge on the application of the DMA in private disputes and to allow the Commission to provide written and oral observations to Dutch courts. Hungary's Competition Act provides that a copy of the final judgment decided by a national court should be transmitted to the Commission. Latvia also amended its Civil Procedure Law for DMA matters.

	DSA	DMA
Austria	No specific measures, so cooperation would rely on Art. 82 DSA. There are general procedural rules not related to the DSA but that can be applied.	No specific measures, so cooperation would rely on Art. 39 DMA.
Belgium	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Bulgaria	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Croatia	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA. There are rules about cooperation between courts contained in the Competition Act.
Czechia	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Denmark	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Finland	The Act on the Publicity of Court Proceedings in General Courts sets out: – A trial document is public unless it needs to be kept secret for a listed reason or because of a court order The Act on the Publicity of Administrative Court Proceedings sets out: – Provisions of the Act on the Openness of Government Activities and other legislation apply to the publicity and confidentiality of court documents, unless otherwise stipulated in the Act	No specific measures, so cooperation would rely on Art. 39 DMA.
France	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Germany	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Greece	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Hungary	N/A	The court issuing the decision sends a copy of the final judgment to the National Office, who forwards a copy of the final judgment without delay to the Minister responsible for Justice for transmission to the Commission.

Italy	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Latvia	– Decisions of the DSC may be appealed before the Administrative District Court – Decisions cannot be challenged before the DSC, only in appeal – The Commission has the right to submit written or oral observations to the national courts – The DSC carry out its tasks unless the Commission has initiated proceedings	– Cases concerning breaches of DMA are to be heard by the Economic Court of the Republic of Latvia in accordance with civil procedure – Upon initiating a case, the court must send a copy of the claim and the decision to initiate the case to the competition authority in 7 days – After the judgment, the Economic Court must send a copy of it to the competition authority and the Commission in 7 days. – (proposed) the Economic Court must suspend proceedings if there is an ongoing investigation by the competition authority or Commission. – The Economic Court's decisions must not be contradictory to the Commission's decisions.
Lithuania	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Netherlands	No specific measures, so cooperation would rely on Art. 82 DSA.	General Civil Procedural Code was amended: – Civil courts can judge on the application of the DMA in private disputes – Commission is allowed to provide written and oral observations to Dutch courts (Art. 39 DMA)
Norway	The DSA does not yet apply in Norway, but the submission of written observations as provided for in Article 82(2) could also be based on provisions of the Norwegian Dispute Act.	The DMA does not yet apply in Norway, but the submission of written observations as provided for in Article 39(3) could also be based on provisions of the Norwegian Dispute Act.
Poland	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Portugal	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.
Romania	No specific measures, so cooperation would rely on Art. 82 DSA.	No specific measures, so cooperation would rely on Art. 39 DMA.

Slovakia	Administrative Procedure Code sets out: – Commission is allowed to be heard before the court and submits its observations – Court has to allow access the Commission access to court files and documents – Court is bound by a decision from the Commission	
Slovenia	No specific measures, so cooperation would rely on Art. 82 DSA.	Rules that apply to competition law and which apply to the DMA by extension: – Where the Commission issues a decision based on Art. 101 or 102 TFEU, the court must send a copy of the written opinion to the competition law agency and parties – The competition law agency may submit written opinions to the court – Where the competition law agency gives a written opinion based on Art. 101 or 102 TFEU, it must send a copy to the Commission – The court itself may request the opinion of the Commission – in such a case, it must inform the parties thereof and, upon receipt of the opinion, send a copy of the opinion to the competition law agency and the parties to the proceedings.
Spain	N/A	No specific measures, so cooperation would rely on Art. 39 DMA.
Sweden	No specific measures, so cooperation would rely on Art. 82 DSA.	N/A

Question 3. National authorities and the DMA

Are there areas of the DMA (e.g., particular obligations or categories of core platform services) for which you consider that the role of national competition authorities is or is likely to be particularly useful in bringing to the attention of the Commission information about possible non-compliance with the DMA under Article 27 DMA?

Croatia answered that their competition authority might be able to provide valuable insight in the tourism sector for core platform services, while Spain stated that their competition authority will be useful in four different types of core platform services (online advertising services, online social networking services, online intermediation services, and number-independent interpersonal communication services).

Austria, Germany, the Netherlands, and Portugal have reported that their competition authorities could be useful in filtering and investigating potential breaches of the DMA.

	Areas
Austria	The competition authority could be useful in 2 ways: – Subordinate role to the Commission where there is a potential breach of the DMA – Filtering role by sorting cases that are solely to do with antitrust law and not the DMA.
Belgium	N/A
Bulgaria	It can be assumed that the competition authority can signal to the Commission valuable information and important cases on misleading information dispersed via platform services.
Croatia	It is unlikely that the competition authority will be particularly useful in bringing to the Commission's attention information about possible non-compliance. However, it might provide valuable insight in the tourism sector for core platform services.
Czechia	N/A
Denmark	Cooperation could be particularly useful for: – Assessment of technical details – Requirements related to data access
Finland	N/A
France	The competition authority issued 2 opinions on: – Competitive operation of cloud computing – Competitive operation of the generative artificial intelligence sector
Germany	The competition authority can be useful in 2 ways: – Act as a filter and messenger, by forwarding information to the Commission – As a first point of contact for information from commercial users, competitors or end users.
Greece	N/A
Hungary	N/A
Italy	N/A
Latvia	The competition authority is well-positioned to monitor compliance with local undertakings. The competition authority is likely to be the first point of contact for companies at risk of violations of the DMA.
Lithuania	It is unlikely that the competition authority will be particularly useful in bringing to the Commission's attention information about possible non-compliance.
Netherlands	The competition authority will be useful: – By filtering and investigating complaints on behalf of the Commission – With its knowledge of the competition sector in the Dutch context – With its experience in enforcing competition law in digital markets

Norway	N/A
Poland	No areas are identified.
Portugal	The competition authority can be useful for areas where experience and investigative capacity are essential to identify and report breaches as well as perform and monitoring roles.
Romania	No areas are identified.
Slovakia	No areas are identified.
Slovenia	No areas are identified.
Spain	The competition authority will be useful in 4 different types of core platform services: – Online advertising services – Online social networking services – Online intermediation services – Number-independent interpersonal communication services Regarding enforcement, the competition authority is also knowledgeable in competitive dynamics of online intermediation services, with experience in sanctioning Amazon and Apple.
Sweden	As there are large tech firms in Sweden, they may provide tips. Game developers who conduct transactions through platforms could become relevant.

Section 4: Private Enforcement of the DSA/DMA

Question 1. National experience

In your Member State, can you observe any actions brought by private parties before national courts to enforce the provisions of the DSA or DMA? If so, please describe the relevant experience.

Only a few Member States reported actions before national courts to enforce the DSA. Germany had a case dealing with Articles 54, 16, and 20 of the DSA. There is also an ongoing case against Etsy for various breaches of transparency obligations. The Netherlands reported a case involving Articles 12 and 17 in the context of shadow banning, and a case involving Articles 16 and 23 of the DSA in the context of intellectual property infringement.

No specific actions were reported concerning the DMA.

	DSA	DMA
Austria	Several cases relating to: – Provision of information data for the purpose of clarifying a concrete suspicion of a defamation offense – Claims for injunctive relief against the dissemination of content infringing personal rights with effect for Austria, Germany, and Switzerland and how the DSA affects the assessment of the applicable law – International jurisdiction regarding claims for information against a service provider in the context of the Brussels I Regulation – Exclusions of liability standardized in Art. 4 DSA in relation to the national law	No actions.
Belgium	No actions.	No actions.
Bulgaria	N/A	N/A
Croatia	No actions.	No actions.
Czechia	No actions.	No actions.
Denmark	No actions.	No actions.
Finland	N/A	N/A
France	No actions.	No actions.
Germany	Only a small number of published court decisions: – One case that dealt with Art. 54, 16, and 20 DSA[a)] – Some cases addressed the question of future regulations under the DSA and their retroactive effect (but did not answer the question)[b)] There is also an ongoing case against Etsy for various breaches of transparency obligations.[c)] The action against TEMU has been withdrawn.[d)]	It can be assumed that there are pending actions, especially with the recent waves of actions against large platform companies in Germany.
Greece	No actions.	No actions.
Hungary	No actions.	No actions.

[a)] LG Berlin, judgment of November 21, 2023 – 27 O 97/22.
[b)] E.g. OLG Dresden, judgement of December 5, 2023 – 14 U 503/23.
[c)] https://www.wettbewerbszentrale.de/wettbewerbszentrale-klagt-gegen-etsy/
[d)] https://www.wettbewerbszentrale.de/dsa-verfahren-temu-verpflichtet-sich-zur-unterlassung/

Italy	N/A	No actions. However, the gap in the adoption of specific private enforcement rules for the DMA makes it harder to detect pending cases.
Latvia	No actions.	No actions.
Lithuania	No actions.	No actions.
Netherlands	2 cases relating to: – An X user claimed to have been shadow banned and Art. 12 and 17 DSA were breached by the provider in doing so.[e] – Erasmus University sought a technical remedy whereby a note-sharing website would take action to prevent infringement of the University's intellectual property, but the Court explained that Art. 16 and 23 DSA were not breached, as there is no obligation to filter content beforehand.[f]	N/A
Norway	No actions because the law is not yet implemented.	No actions because the law is not yet implemented.
Poland	No actions. There is proposal for the adoption of provisions relating to civil law claims of service recipients affected by an infringement of the DSA.	No actions.
Portugal	No actions.	No actions.
Romania	No actions.	No actions.
Slovakia	N/A	N/A
Slovenia	N/A	N/A
Spain	No actions.	No actions.
Sweden	No actions.	No actions.

[e] Amsterdam District Court, July 5, 2024, ECLI:NL:RBAMS:2024:3980, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:3980

[f] Amsterdam District Court, July 24, 2024, ECLI:NL:RBAMS:2024:4425, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:4425&showbutton=true&keyword=Studeersnel&idx=1

Question 2. Causes of action and likely litigation of the DSA

What are the actual or expected causes of action under national law to privately enforce the DSA? What are their limits and opportunities? How likely is the use of private redress, including collective redress or contract law, in your Member State to enforce the DSA? What type of actors do you expect to be most likely to engage in private enforcement?

Many Member States identified the difficulty of proving the existence of a breach or proving the extent of damages as a potential limitation. Another limitation mentioned by Member States is the fact that parties might be deterred from filing a lawsuit because such difficulty to demonstrate the damages and because of the costs and hassle. Most answers to the question on opportunities focused on collective procedure.

Among the Member States who answered positively to the likelihood of private redress, most specified that collective redress would be most likely.

In regard to the types of actors to be most likely to engage in private enforcement, most Member States mentioned intermediary services providers, while Slovakia and Slovenia answered consumer organisations.

	Causes	Limits and pportunities	Likeliness of private redress	Types of actors
Austria	Basis: – Art. 14, 16, 17, 20, and 21 DSA Causes – Disclosure of user data Injunctive relief and removal due to violation of personal rights, specifically for online hate speech – Damages and losses	Limits: – Proving the existence of a breach might be difficult because general rules of evidence apply – Parties might be deterred from filing a lawsuit, especially in the case of scattered damage, because of the low claims and high risk Opportunities: – Class actions could be a better form of redress	N/A	Intermediary service providers Service users
Belgium	N/A	N/A	N/A	N/A

Bulgaria	N/A	N/A	Private enforcement is unexplored under national law.	N/A
Croatia	Basis: – Art. 9, 10, 21, 22, 51(1)-(3), 53 DSA	N/A	N/A	Intermediary service providers Service users
Czechia	Basis: – Competition or consumer protection Causes: – Non-consensual use of personal data	Limits: – Costs and hassle of individual private lawsuits Opportunities: – The recent adoption of the Act on Collective Civil Court Procedure might encourage more private enforcement – Out-of-court dispute resolution as an alternative	Not likely before the adoption of the implementing act. Even after the adoption, public enforcement is more likely.	N/A
Denmark	Causes: – Contesting competent authority's decisions or failure to act – Violation of the DSA	N/A	Complaints to the competent authority are more likely than lawsuits.	Business organisations
Finland	No specific rules for private enforcement, so general rules apply.			
France	Basis: – Intellectual property – Competition	N/A	N/A	Intermediary service providers Service users
Germany	Causes: – Art. 25 DSA – Art. 54 DSA – Violations of personality rights	N/A	Private redress is likely regarding violations of personal rights.	Individual users Business users Competitors
Greece	Basis: – Civil tort based on unfair competition	N/A	N/A	Service providers only on the basis of civil tort

Hungary	Basis: – Liability in tort for incompliance with the DSA Causes: – Interference with fundamental rights – Limiting access to resources for market players – Content interfering with the plaintiff's rights	Opportunities: – National tort law is flexible, and a great variety of cases are possible – Another remedy available is prohibiting the service provider from the behaviour that threatens by causing damage, which can be combined with an injunction order	N/A	N/A
Italy	Causes: – To oblige the service provider to comply with the DSA – To recover damage caused by failure to comply with the DSA	Opportunities: – New Art. 840 of Civil Procedure Code provides that non-profit organizations or organizations whose objective is the protection of individual rights or members of a class action can file a lawsuit against a public services provider, which might facilitate actions as opposed to individual actions	N/A	N/A
Latvia	– Contractual breaches – Non-compliance with consumer protection regulations	Limitations: – Establishing causation or demonstrating a direct link between the non-compliance and the harm suffered can complex – Obtaining such evidence can be challenging due to the technical compleity of digital services and the often cross-border.	Collective actions are likely	Businesses Consumers

		Nature of the digital service providers Opportunities: – A decision on interim relief may be taken by the DSC based on a prima facie finding of an infringement where it has reason to believe that the recipients of the service provided by online intermediary are likely to suffer significant harm and urgent action there is required		
Lithuania	Basis: – Intellectual property	N/A	Not likely, as private collective redress are not developed in Lithuania.	N/A
Netherlands	Causes: – Claims for damages based on tort law or unjust enrichment – Preliminary injunctions – Claims for condemnatory relief – Claims for declaratory relief – Nullity of contracts	Limits: – For damage-based claims, it will be hard to prove and quantify damages, demonstrate a causal link between the infringement and the damages	Likely Mass or bundled actions are more likely than individual actions because of the cost of litigation	Business users End users
Norway	N/A	Limits: – Class actions might be hard to finance because it relies on an opt-out model where class members cannot be held liable for legal costs or remuneration of the class representative	N/A	N/A

Poland	Causes: – Compensation for damages – Compensation for violation of personal rights – Contractual liability and compensation for breach of contract	N/A	Some possibilities offered by the law on collective redress amended in 2024 to facilitate consumers bringing collective actions.	Based on a recent case pre-DSA: – NGOs – Associations – Service providers
Portugal	Causes: – Extracontractual liability – Injunctions – Collective actions	N/A	Currently, collective redress is not common.	N/A
Romania	N/A	N/A	N/A	N/A
Slovakia	Anticipated: – Claims for damages	N/A	Unlikely	Consumer organisations
Slovenia	Basis: – Tort law – Contract law – Consumer protection law – Data protection law Causes: – Claims for damages due to infringement of the DSA – Breach of contractual obligation	Limits: – Proving the existence of damages	Collective actions are more likely than individual actions.	Consumer organisations

Spain	Basis: – Non-contractual liability – Consumer law – Unfair competition	Opportunities: – For collective complaints, there are two paths available simultaneously: representation regarding the responsibility of intermediary service providers (Art. 86 DSA) and representation regarding consumer rights (Directive 2020/1828)	N/A	N/A
Sweden	N/A	N/A	Private redress is likely to be limited.	N/A

Question 3. Causes of action and likely litigation of the DMA

What are the actual or expected causes of action under national law to privately enforce the DMA? What are their limits and opportunities? How likely is the use of private redress in your Member State? What type of actors do you expect to be most likely to engage in private enforcement?

Similar to the DSA, most Member States answered that a limitation is the quantification and proof of damages. Austria and Germany also identified the risk of national courts and the Commission arriving at divergent interpretations.

Out of the twenty-three Member States, nine answered that the use of private redress was unlikely. Member States who answered private redress was likely mentioned different circumstances. Namely, Austria mentioned that follow-on actions are more likely, while Germany mentioned that actions led by consumer associations are probably going to become more relevant.

Among the types of actors that were named, competitors, end users, and consumer organisations were identified.

	Causes	Limits and Opportunities	Likeliness of private redress	Types of actors
Austria	Basis: – Tort law – Unfair competition Causes – Claims for damages – Injunctive relief	Limits: – Determining and quantifying damages – For stand-alone actions (as opposed to follow-on actions): risk of different interpretations of the DMA provisions by the Commission and national courts	Follow-on actions are more likely	Competitors of gatekeepers
Belgium	N/A	N/A	N/A	N/A
Bulgaria	N/A	N/A	Private enforcement is unexplored under national law.	N/A
Croatia	N/A	N/A	N/A	N/A
Czechia	Basis: – DMA – Competition laws, e.g., TFEU or national law	N/A	Unlikely, given that private enforcement will probably be at the EU level and not the national level	N/A
Denmark	Causes: – Contesting competent authority's decisions or failure to act – Violation of the DMA	N/A	Complaints to the competent authority are more likely than lawsuits.	Business organisations
Finland	No specific rules have been adopted for private enforcement, so general rules apply.			
France	N/A	Limits: – Evaluation of damages	Likely because: – There is already private enforcement under Art. 102 TFEU – 20 years of experience in competition law enforcement means lawyers, counsels, judges, etc. are	Businesses

			better equipped to deal DMA enforcement – Applying prohibitions per se will be easier than prohibitions based on unfair competition – CJEU might see private enforcement as an essential pillar for DMA enforcement.	
Germany	Injunctions are expected to become more relevant. Preliminary rulings from German civil courts and CJEU are likely to have a special role in the context of legal uncertainty. As opposed to antitrust law, follow-on actions are not likely for the DMA, because violations are practiced openly and are addressed by the Commission quickly.	Limits: – Art. 5-7 DMA are not interpreted uniformly by courts – Lack of guidance from the Commission's decision-making practice or procedures might lead to national judges arriving at different interpretations – Proving causal damage in civil proceedings	Likely, because the evidence requirements are lower than traditional abuse control. Collective redress is not likely to become relevant. Redress action led by consumer associations is more likely to become relevant (Art. 42 DMA).	Competing service providers End users
Greece	Basis: – Competition law – Tort law	N/A	N/A	Competitors Users

Hungary	Causes: – Damages action	Limitations: *See next column.*	Unlikely because proving the causal link and the amount of loss resulted from the violation of the DMA may create obstacles for bringing claims before courts.	N/A
Italy	N/A	N/A	Unlikely for the time being, because private enforcement of the DMA has not yet been regulated	N/A
Latvia	N/A	N/A	Unlikely	End users and business users of core platform services
Lithuania	N/A	N/A	Unlikely because private enforcement is rarely used in competition cases	N/A
Netherlands	Causes: – Claims for damages based on tort law or unjust enrichment – Preliminary injunctions – Claims for condemnatory relief – Claims for declaratory relief – Nullity of contracts	Limits: – For damage-based claims, it will be hard to prove and quantify damages, demonstrate a causal link between the infringement and the damages – Information is often kept by gatekeepers and not accessible – The cost of quantifying damages might deter parties	Likely Mass or bundled actions are more likely than individual actions because of the cost of litigation	N/A
Norway	*See Question 2.*			

Poland	N/A	N/A	Unlikely Although the law on collective redress was amended in 2024 to facilitate consumers bringing collective actions.	Larger e-commerce platforms that are gatekeepers' business users
Portugal	N/A	N/A	Collective redress is unlikely	N/A
Romania	N/A	N/A	N/A	N/A
Slovakia	Claim for damages	N/A	Unlikely	Consumer organisations
Slovenia	Basis: – Unfair competition – Contract law Claim for damages	Limits: – Private actions might be limited by the need to align with or wait for the Commission's findings – Proving damages may require complex resources Opportunities: – Introduction of collective actions and growing role of the EU in regulating digital markets could encourage more private actions	Unlikely, because there are no gatekeepers established in Slovenia.	Businesses that rely on digital platforms Consumer associations
Spain	Causes: – Violation of one of the DMA provisions – (Once it is transposed in the national law) collective action through the Representative Actions Directive (Art. 42 DMA) Basis: – Non-contractual liability	Opportunities: – A private party can take action against other private parties (e.g., gatekeepers) for breach of other laws to demonstrate unfair competition	Not likely, because of the leeway the DMA allows for forum shopping	Consumers Business users
Sweden	N/A	N/A	N/A	Competitors

Question 4. Specific rules for the DSA/DMA

Have any specific national rules been adopted (or planned for adoption) for private enforcement of either DMA/DSA (e.g., taking inspiration from the national rules transposing the antitrust Damages Directive)? Is there any plan to allocate cases concerning the DMA/DSA to a specific court or chamber and if so, which one?

Concerning the DSA, only France reported that some measures have been amended for the DSA and Poland mentioned proposals for the adoption of measures. Concerning the DMA, only Germany reported that specific rules have been extended to the application of the EU Regulation.

While most Member States do not have a specific court or chamber, Lithuania, Norway, and Slovenia have designated a court. Germany designated a court for DMA matters and mentioned the possibility of DSA disputes falling within a court's area of specialization. Latvia also proposed to designate a court for DMA matters.

	Specific Rules	Specific court or chamber
Austria	DSA: no specific rules. DMA: no specific rules, but regulations based on the German model have been proposed and regulation at EU level based on the Damages Directive has been considered.	DSA: no specific court, except for information orders which go to the Court of First Instance.
Belgium	N/A	N/A
Bulgaria	DSA: According to the bill, the DSC is designated to certify out-of-court resolution bodies. DMA: N/A.	The Sofia City Administrative Court is designated as competent to order measures for removal of content.
Croatia	DSA: No specific rules. DMA: N/A	N/A
Czechia	No specific rules.	Unlikely that there will be specific courts or chambers designated. With the Collective Civil Procedure Act, the Municipal Court in Prague has sole jurisdiction for collective claims, which could include the DSA and DMA.
Denmark	No specific rules.	No specific courts.
Finland	No specific rules.	No specific courts.

France	DSA: the following provisions have been amended: – Concerning the role of courts relating to online communication to the public – Concerning measures to stop or prevent damage caused by the content of an online public communication service DMA: no specific rules, but a law on collective action has been proposed which would include DMA breaches.	N/A
Germany	DSA: No specific rules. DMA: provisions concerning private enforcement of antitrust law based on the Antitrust Damages Directive have been partially extended to the DMA – Parties are entitled to claims for removal and injunctive relief – Parties are entitled to claim compensation – Decisions from the Commission are binding in regard to violations and appointment of gatekeepers – Possible to order the publication of binding decisions from authorities – Parties can claim for the disclosure of evidence and provision of information against the gatekeeper – Federal Cartel Office is allowed to intervene as an "amicus curiae"	DSA: No specific court, but there might be a regional court and a higher regional court designated if DSA-related disputes fall under a specialized area. DMA: antitrust chambers of regional courts have jurisdiction for DMA disputes.
Greece	No specific rules.	No specific court. However, the Court of First Instance in Athens and Thessaloniki has exclusive competence for data protection and e-communication.
Hungary	No specific rules.	No specific court.
Italy	DSA: N/A DMA: no specific rules. However, the Associazione Italiana Giuristi Europei has requested the implementation of specific rules.	DSA: N/A DMA: no specific court.

Latvia	No specific rules.	DSA: N/A DMA: (proposed) Economic Court of the Republic of Latvia
Lithuania	No specific rules.	The administrative courts will be competent.
Netherlands	No specific rules.	N/A
Norway	No specific rules, proposed or adopted. The Damages Directive has not yet been incorporated into the EEA Agreement, so it could not serve as a model. Nonetheless, private enforcement of competition law does take place, which could be the same for the DSA and DMA.	Some specialised courts and specialised out-of-court dispute resolution bodies exist in specific fields, e.g., relating to consumer disputes.
Poland	DSA: following rules have been proposed: – Interrelations between civil and administrative proceedings – Competent authorities may present opinions to the courts, if it is of public interest – Courts should inform the competent authorities about the claim and about the binding rulings DMA: No specific rules, proposed or adopted. However, there are discussions to broaden the application of the national law implementing the Damages Directive to the DMA.	DSA: (proposal) regional courts for matters of Art. 54 DSA. DMA: no specific court.
Portugal	No specific rules.	No specific court.
Romania	DSA: no specific rules. DMA: N/A	DSA: no specific court. DMA: N/A
Slovakia	No specific rules. However, the law on collective actions applies.	No specific court.
Slovenia	DSA: No specific rules, proposed or adopted. DMA: No specific rules, proposed or adopted. However, the law on collective actions applies.	DSA: The Nova Gorica District Court has exclusive jurisdiction for requests for the removal of illegal content from the Internet (Art. 9 DSA). Initially, the Ljubljana District Court held exclusive jurisdiction, but due to

		this court's overload of other cases, the exclusive jurisdiction was soon transferred to the District Court in Nova Gorica. Actions against the supervisory authorities' decisions against internet intermediaries in a supervisory procedure may be brought before the Administrative Court of the Republic of Slovenia. DMA: No special court, proposed or adopted. Actions against the competition agency can be brought before the Administrative Court.
Spain	DSA: N/A DMA: No specific rules, proposed or adopted.	DSA: N/A DMA: No specific court.
Sweden	No specific rules, proposed or adopted.	No specific court.

Question 5. Civil society and interventions

Does the national procedural law allow civil society organisations to intervene in pending private disputes in support of the public interest? If so, how difficult or costly is it, and how does it work?

Only in Lithuania, Slovenia, and Spain, civil society organisations are not allowed to intervene. In most Member States, the criteria for allowing the participation of civil society organisations are a legitimate legal interest and that the case falls within the scope of the organisation. Two Member States indicated that organisations should cover their legal costs, while three indicated the opposite. Norway, Portugal, and Sweden reported that the organisations would pay only where the case is not successful.

	Allowed	Criteria	Difficulty or cost	How it works
Austria	Yes.	Legal interest that goes beyond a mere economic and public interest.	Costs are covered by litigation funding or state subsidies. A fee can be agreed upon, that may not exceed EUR 250.00 and 20% of the amount of the claim.	N/A
Belgium	Yes.	Interest corresponds to the organisation's corporate purpose and aims at protection human rights or fundamental freedoms.	N/A	N/A
Bulgaria	No.	N/A	N/A	N/A
Croatia	Yes.	Legitimate interest and relevance.	Organisations may have to bear the procedural costs.	1. Organisation files a request to the court 2. Court evaluates the organisation's standing and interest 3. Possibility to appeal the court decision
Czechia	Yes.	Legal interest that is beyond a moral or general interest.	N/A	1. Organisation notifies the court of their intention to intervene. 2. The party must consent to the intervention. In the cases of collective actions, consumer associations are meant to initiate the dispute on their own.
Denmark	Yes.	Legal interest.	The costs might be covered by the organisation or by the parties, depending on the outcome of the case.	Organisation submits a written or oral application to the court. The court decides how the intervener may participate in the case and if it allowed to submit evidence.

Finland	Yes, but it is the exception.	The matter concerns their rights and plausible reasons are presented.	N/A	N/A
France	Yes, to intervene or initiate.	N/A	N/A	N/A
Germany	Yes.	Legal interest, which is not simply economic, idealistic or an actual interest, or the interest of others.	No costs incurred by the court, but there might be attorney fees.	The organisation can perform all procedural acts if they do not contradict the declarations and actions of the main party. The intervention is declared by a written statement submitted to court.
Greece	Yes, but only in consumer protection and data protection cases.	N/A	N/A	N/A
Hungary	Yes.	They do not have the right to claim for damages; they can only submit claims for public interests.	N/A	N/A
Italy	Yes.	N/A	N/A	N/A
Latvia	N/A	N/A	N/A	N/A
Lithuania	No.	N/A	N/A	N/A
Netherlands	Yes, pursuant to the Representative Actions Directive.	N/A	N/A	N/A

Norway	Yes. They are also allowed to submit observations without intervening.	If the case falls under the purpose and normal scope of the organisation.	If the action is successful, the legal costs might be covered by the opposing party. If the action is unsuccessful, the organisation might be liable to cover the legal costs of the opposing party. In the case of submitting only observations, the organisation must support its own costs and is not liable for costs from the opposing party.	1. Intervention is declared to the court and must be motivated. 2. Parties may contest the intervention.
Poland	Yes, to intervene or initiate.	The case must be within the organisation's statutory goals. It can only be in relation to: – Consumer protection – Environment – Industrial property – Equality and non-discrimination	Organisations are exempt from court proceedings costs.	N/A
Portugal	Yes, through voluntary joint litigation.	The case is to protect constitutional interests. The case is within the organisation's purpose.	If the case is successful, the organisation does not pay the costs. If the case is not successful, the organisation will pay between 1/10 and 1/2 of the costs.	1. The organisation submits an application to the court. 2. The organisation can accept the case as it stands when it joins.

Romania	Yes.	Legal interest.	The organisation will need to cover the cost of the stamp for the request.	1. The organisation submits a request to the court. 2. If the request supports the public interest, it will be qualified as an accessory request which can be filed at any times throughout the trial before the closing of debates.
Slovakia	Yes.	In support of public interest.	N/A	The court might bring in the organisation without motion if the main party agrees. For consumer associations, it needs to be on the List of Entitled Persons to be allowed to initiate a collective action.
Slovenia	No.	N/A	N/A	N/A
Spain	No.	N/A	N/A	N/A
Sweden	Yes	N/A	The losing party bears the costs.	N/A

Section 5: General Questions

Question 1. Orders under the DSA

Did your Member State specifically implement Articles 9 and 10 of the DSA in the national law? And if yes, in what way, and why? Does the national law specifying injunctions according to Articles 4(3), 5(2) and 6(4) meet the requirements of oversight by authorities or courts? Are there any specific rules, or cases in this regard in your jurisdiction?

Regarding the implementation of Articles 9 and 10 of the DSA, five Member States specifically implemented them in their national law, and Slovakia and Slovenia only did for Article 9. Six Member States implemented the articles

only by referring to the DSA in their national laws, and six Member States did not implement the articles.

Many Member States reported that Articles 4(3), 5(2) and 6(4) were not implemented in their national law. The ones that did implement the articles reported that the national law met the requirements of oversight.

	Implementation of Art. 9 and 10 DSA	Does the law meet the requirements of oversight?	Specific rules or cases
Austria	The national E-Commerce Act already contained provisions which regulate orders of Art. 9 and 10 DSA.	Yes, as these injunctions were already implemented in the national law with the E-Commerce Directive.	Because cases of hate online are often cross-borders, the national law has specific rules for these cases.
Belgium	N/A	N/A	N/A
Bulgaria	N/A	N/A	N/A
Croatia	They are transposed in the implementing act: – Competent authorities to issue orders are designated – Authorities have to issue the orders ex officio – Content of the orders is not directly regulated but rather refers to the DSA – The delivery time is recorded as the time when the order has been sent	Injunctions issued by courts: Yes, they would be subject to ordinary judicial oversight. Injunctions issued by competent authorities: Yes, they would be subject to administrative judicial oversight.	There have been multiple cases on the constitutionality of the General Administrative Procedures Act and the conclusions have been that the law meets the criterion of effective judicial oversight and right to a fair trial.
Czechia	They are transposed in the draft implementing act: – There are requirements for the content of orders in general and for criminal proceedings	Art. 4(3), 5(2), and 6(4) DSA are not implemented in the draft implementing act.	N/A
Denmark	They are transposed in the implementing act, which refer to the requirements of Art. 9(2) and 10(2) DSA.	Art. 4(3), 5(2), 6(4) DSA are not implemented in the implementing act.	N/A

Finland	They are transposed in the implementing act, which refer to Art. 9 and 10 DSA. Provisions of the PECSA, the law implementing the E-Commerce Directive, which was after modified by the DSA, also contains provisions regarding to information orders.	N/A	N/A
France	They are transposed in the implementing act: – Search, investigation, injunction and penalty powers of the Arcom are defined – Arcom can collect undertakings from platforms which would become mandatory and require that action plans are submitted – Arcom can request the court to order a temporary restriction order to access a provider – Arcom can issue monetary sanctions if injunctions are not followed	Arcom's decisions regarding injunctions can be contested before the State Council.	*See first column.*
Germany	They have not been implemented.	Art. 4(3), 5(2), 6(4) DSA are not implemented in the implementing act.	N/A
Greece	They are transposed in the implementing act, which refer to Art. 9(2) and 10(2) DSA.	They meet the oversight requirements.	N/A
Hungary	N/A	N/A	N/A
Italy	They have not been implemented.	N/A	N/A

Latvia	The Cabinet of Ministers shall be authorized to issue legal acts to regulate on: – Information to be specified in the decision referred to in Art. 9 DSA – Procedure for attaching an annex to the decision referred to in Art. 9 DSA where the decision relates to the restriction of multiple online resources – Time limit for the execution and operation of the decision referred to in Art. 9 DSA – Conditions and procedure for the inclusion of the information contained in the decision referred to in Art. 9 DSA or in an annex in a machine-readable list maintained by the authority – Procedure for communicating the decision referred to in Art. 9 or the request for information referred to in Art. 10 DSA and information on the execution thereof to the DSC	N/A	N/A
Lithuania	They are implemented in the national law only by reference.	N/A	The authorities must obtain approval from the administrative court before issuing orders.
Netherlands	They have not been implemented because of their direct effect.	N/A	When orders originate from criminal law, Art. 9 (3)-(5) and 10(3)-(5) can be put aside.
Norway	N/A	N/A	N/A

Poland	They are transposed in the draft implementing act, but it is still under discussion.	N/A	N/A
Portugal	They have not been implemented.	Art. 4(3), 5(2), 6(4) DSA are not implemented in the implementing act.	N/A
Romania	They are transposed in the implementing act.	Decisions taken pursuant to Art. 4(3), 5(2), 6(4) DSA are overseen by at least one court.	N/A
Slovakia	Art. 9 was transposed in the implementing act to complement the existing law on: – Identification and localisation information – Information on legal basis – Information on territorial scope – Information on public administration bodies – Delivery through electronic contact points – Establishment of a special time period to submit objections against decisions on the prevention of the dissemination of illegal content	Art. 4(3), 5(2), 6(4) DSA are not implemented in the implementing act.	N/A
Slovenia	Art. 9 is transposed in the implementing act.	N/A	The implementing act adopts a graduated approach to the choice of possible measures for removing illegal content which can be imposed on hosting providers, mere conduit providers, registries, and domain registrars.

Spain	The implementing act refers to Art. 9 and 10 DSA, but fails to incorporate in a right way the spirit of the articles and the referral is included in the wrong place in the national legislation	Art. 4(3), 5(2), 6(4) DSA are not implemented in the implementing act.	The DSC now has the power to transmit a copy of the orders to act against illegal content or the delivery of information received by it to other DSCs.
Sweden	The implementing act refers to Art. 9 DSA	N/A	The implement act provides that: – Decisions made by supervisory authorities may be appealed when they are made under the DSA, legal acts adopted pursuant to the DSA, the implementing act, or regulations in connection – Appeals to the Administrative Court of Appeal require leave to appeal

Question 2. Legal representatives under the DSA

Are you aware of the services of legal representatives according to Article 13 DSA being provided in your Member State? If so, please describe the situation.

Only Austria, Belgium, Germany, and the Netherlands have reported that legal representatives were appointed by service providers in their countries.

	Appointment of Legal Representatives
Austria	Only one service provider has appointed legal representatives.
Belgium	These intermediary service providers had appointed legal representatives: – Telegram – Samsung Electronics
Bulgaria	No legal representatives appointed.
Croatia	No legal representatives appointed.
Czechia	No legal representatives appointed.
Denmark	No legal representatives appointed.
Finland	N/A
France	No legal representatives appointed.

Germany	There are already providers that have legal representatives available for communication and coordination with supervisory authorities.
Greece	N/A
Hungary	No legal representatives appointed.
Italy	No legal representatives appointed.
Latvia	No legal representatives appointed.
Lithuania	No legal representatives appointed.
Netherlands	Several have appointed legal representatives. Their contact details must be shared with the DSC. They will be consulted by the competent authorities or the Commission concerning compliance with the DSA.
Norway	N/A
Poland	No legal representatives appointed.
Portugal	No legal representatives appointed.
Romania	No legal representatives appointed.
Slovakia	N/A
Slovenia	No legal representatives appointed.
Spain	No legal representatives appointed.
Sweden	No legal representatives appointed.

Question 3. National DSA complaints

Did the national law adopt any specific approach vis-a-vis complaints according to Article 53 of the DSA? (e.g., limiting them only to systemic violations)

Only Denmark, France, and Poland have reported that their national laws adopt a specific approach.

	Specific Approach
Austria	No specific approach.
Belgium	No specific approach.
Bulgaria	No specific approach.
Croatia	No specific approach. The approach is rather perfunctory.
Czechia	No specific approach.
Denmark	The authority can reject complaints without further assessment. There is no possibility to appeal the decisions of authorities before a higher public authority, only before national courts. The Minister for industry, business and financial affairs can adopt rules on submission of complaints.

Finland	No specific approach.
France	The tripartite agreement between the Arcom, CNIL and DGCCRF regulates cooperation between the authorities for handling complaints.
Germany	The DSC is the central and sole body receiving complaints. No further specific approach.
Greece	No specific approach.
Hungary	No specific approach.
Italy	N/A
Latvia	The DSC will deal with complaints according to the procedure laid down in the Law on Submissions,
Lithuania	No specific approach.
Netherlands	No specific approach.
Norway	N/A
Poland	Although the complaints are not limited to systemic infringements, the general approach focuses on systemic infringements.
Portugal	No specific approach.
Romania	No specific approach.
Slovakia	No specific approach.
Slovenia	No specific approach.
Spain	N/A
Sweden	No specific approach.

Question 4. Political controversy of the DSA/DMA

Were the DSA or DMA subject to political controversy during the implementation on the national level, and if so, why?

Criticism for the DSA and DMA varies among the different Member States.

Concerning the DSA, four Member States identified controversy surrounding the lack of clarity regarding the competent authorities' powers. Two Member States mentioned the orders to act against illegal content as a point of contention.

Concerning the DMA, two Member States reported that the lack of enforcement powers for their competent authorities drew criticism.

	Political Controversies
Austria	No controversies for the DSA, but there was criticism for: – Data protection provisions – Information mechanism for removal orders (Art. 9 DSA) – Lack of clarity on the provisions on which individuals can rely to assert their claims No controversies for the DMA, but there was criticism for: – Individual deadlines for the designation procedure should be shortened in order to speed up the process – Greater account should be taken of the customer need for customizability of contracts and facilitation of a change of provider – Interoperable cloud infrastructure components should be more widely used and consideration should be given to avoid lock-in effects and promoting offers – Taxation of the digital sector and online platform work should not have been excluded
Belgium	N/A for the DSA. No controversies for the DMA.
Bulgaria	No controversies yet.
Croatia	No controversies for the DMA. For the DSA, there were 2 issues: – The lack of clear division of jurisdiction among the different authorities – The lack of clarity concerning the extent of the powers of HACOM (DSC) to issue take down notices for illegal content during elections
Czechia	No controversies for the DMA and the DSA.
Denmark	For the DSA, there was criticism concerning: – Provision which states that when handling complaints, the authority should rely on the purpose of the DSA to prioritise or not complaints – which showed a lack of clarity according to some – Derogation of the Law on Access to Documents – which was not necessary according to some – The designation of a single competent authority – which could lead to some issues where the subject matter is also within the scope of the competence of other authorities For the DMA, there was criticism concerning: – Provision that grants the competent authority the right to request all necessary information and require explanations – lack of clarity and wide discretion was criticized by some – Derogation from the Law on Access to Documents – which was not necessary according to some – Provision granting the right to the competent authority to impose daily or weekly fines for supplying information that is incorrect, incomplete or not within the deadline – it was not necessary because the – Commission is the sole enforcer and the fine level appears to be high

Finland	No controversies for the DMA and the DSA.
France	The DSA was criticized for not regulating platforms strictly enough and for allowing extra-judiciary censoring practices. The DMA was criticized for undermining legal certainty and stifling innovation.
Germany	No controversies for the DSA. For the DMA, there was criticism concerning: – Lack of enforcement powers of the Federal Cartel Office – Decentralized law enforcement involving national competition authorities is called for – The continued application of a provision of the Act Against Restraints of Competition which clashed or overlapped with the Art. 1(5) and (6) DMA – Designated gatekeepers are generally unable to provide objective reasons or legitimate interests or efficiencies to justify prima facie unlawful conduct with regard to DMA violations
Greece	No controversies for the DMA and the DSA.
Hungary	No controversies for the DMA and the DSA.
Italy	No controversies for the DMA and the DSA.
Latvia	No controversies for the DMA and DSA. There were some concerns which were addressed during the revisions of the draft law.
Lithuania	No controversies for the DMA and the DSA.
Netherlands	The DSA was criticized for: – Lack of clarity for who determines the illegality of content The DMA was criticized for: – Not leaving a bigger role for national competition authorities
Norway	No controversies for the DMA and the DSA for the time being, apart for the "two pillar challenges" and the potential transfer of authority to ESA and/or the Commission.
Poland	No controversies for the DMA. Under the DSA, the section on legal grounds and national procedures for issuing orders addressing illegal content was subject to controversies raised by NGOs (e.g., Panoptykon) and politicians. Controversies concern excessive powers of Prezes UKE and lack of sufficient judicial control.
Portugal	For the DSA, there is the issue of the lack of clarity concerning the allocation of powers between competent national authorities. No controversies for the DMA.
Romania	For the DSA, the designation of the DSC was presented in some media as the creation of an internet police.
Slovakia	No controversies for the DMA and the DSA.

Slovenia	No controversies for the DMA and the DSA, apart from discussion concerning the designation of an authority to decide on the illegality of content.
Spain	No controversies for the DMA.
Sweden	There was only one referral body that expressed concern for the potential risks of granting the competition authority new powers for the DMA because of the untested nature of the legal framework.

Question 5. Measures to supporting the DSA/DMA ecosystem

Which measures have been taken, or are foreseen, to support the creation of out-of-court dispute resolution bodies, trusted flaggers, DSA/DMA-focused consumer organisations, and data access requests by researchers? Did the national legislature or regulators adopt any specific approaches in this regard?

Concerning the out-of-court resolution bodies and trusted flaggers, many Member States have adopted measures regarding who can qualify, financing, the approval process, and appeal mechanisms.

No Member States have reported any measures adopted for consumer organisations.

For data access requests by researchers, France reported to have set up access for researchers. Germany has published an information page and an application will be made available.

	Out-of-court Dispute Resolution Bodies and Trusted Flaggers	Consumer Organisations	Data Access Requests
Austria	Concerning trusted flaggers, the implementing act provides that: – An application form must be used – KommAustria is responsible for revoking the approval of trusted flaggers – Appeals against revocation decisions have no suspensive effect	No measures.	N/A
Belgium	The selection procedure has not been adopted yet. The implementing act provides that the DSC should indicate which competent authority is responsible for accrediting the applicant.	N/A	Same as out-of-court dispute resolution bodies and trusted flaggers.
Bulgaria	According to the bill, the DSC is designated to certify out-of-court resolution bodies.	N/A	N/A

Croatia	Draft implementing act provides that: – HACOM shall adopt ordinances governing the creation and certification of out-of-court dispute resolution bodies and trusted flaggers within 3 months of the adoption of the implementing act – HACOM shall consult with the competent authority	No measures.	No measures.
Czechia	No measures.	No measures.	No measures.
Denmark	DSA: There are several conditions to be met to become an out-of-court dispute resolution body. DMA: No measures.	N/A	N/A
Finland	Concerning out-of-court dispute resolution bodies, there are no measures. Concerning trusted flaggers, Traficom must notify the approved bodies at the EU level.	N/A	N/A
France	DSA: Concerning trusted flaggers, procedures are currently being drafted. DMA: No measures.	N/A	Arcom has organised its internal interface mission to allow access for researchers.
Germany	DSA: An online form and guide were set up to apply for certification for out-of-court dispute resolution and trusted flaggers. DMA: No measures.	No measures.	An information page has been set up and an application form will be made available.
Greece	No measures.	No measures.	No measures.
Hungary	DSA: Concerning trusted flaggers, the implementing act provides that: – The President of the DSC keeps a register. – The President decides to suspend or revoke the status. – The register is public and available on the DSC's website. Concerning out-of-court dispute resolution bodies, the implementing act provides that:	N/A	The President of the DSC keeps a register. The register is public and available on the DSC's website.

	– They are responsible for attempting to reach an amicable settlement. If unsuccessful, they can make a recommendation. – The body cannot be an administrative authority, and it cannot have judicial or administrative powers. Its procedure is not official procedure. It shall establish its own rules of procedure. – It shall report annually on cases in which the online platform operator has failed to comply with the decision or recommendation. – The rules concerning the initiation of the procedure, the examination of the application, and the proceedings are also provided in the implementing act.		
Italy	Concerning out-of-court dispute resolution bodies, an applicant may already be certified as an ADR body in another sector.	No measures.	No measures.
Latvia	Latvia has decided not to establish out-of-court resolution bodies at this point. There are no trusted flaggers.	No consumer organizations.	No established mechanisms for data access requests.
Lithuania	The CRA has adopted the Description of the supervision procedure for the provision of mediation services provided for in Regulation (EU) 2022/2065, which provides procedures and conditions for applying as an out-of-court dispute resolution body or trusted flagger.	No measures.	No measures yet, but they will be published in the future.
Netherlands	The Ministry of Internal Affairs announced that it is studying the possibility of creating or endorsing with journalists, universities, and other members, a trusted flagger and out-of-court dispute resolution entity. Individuals cannot qualify as trusted flaggers, but associations representing right holders and individual companies can. The Minister is not answering the request to provide more detailed procedures to certify trusted flaggers, out-of-court dispute resolution bodies, and vetted researchers.	N/A	N/A

Norway	No measures.	N/A	N/A
Poland	N/A	N/A	N/A
Portugal	No measures.	No measures.	No measures.
Romania	Measures have been adopted.	N/A	Measures will be adopted in 2025.
Slovakia	No measures.	No measures.	No measures.
Slovenia	The implementing act provides for co-financing of trusted flaggers' activities if deemed necessary (by AKOS). No new measures concerning out-of-court dispute resolution bodies.	N/A	N/A
Spain	Out-of-court dispute resolution bodies: – The DSC can certify bodies and elaborate a biannual report (Art. 21 DSA) – The DSC can grant, suspend and withdraw the condition of a trusted flagger (e.g., Art. 22 DSA)	No measures.	No measures.
Sweden	The establishment of out-of-court resolution bodies is still under discussion.	N/A	N/A

Question 6. Special attention to selected issues

Are there any other specific provisions or issues relating to the DMA/DSA that received particular attention from the side of practitioners (service providers, lawyers, regulators) or academics in your MS, because they are seen as controversial, complex or unclear? If so, please specify. Please limit yourself to issues that may be of relevance from a European perspective.

Various concerns were reported by Member States.

Concerning the DSA, Austria, Denmark, Germany, and Slovenia highlighted issues with delegated acts such as out-of-court resolutions bodies, trusted flaggers, or researchers. Denmark, Poland, and Slovenia noted concerns with the GDPR or other personal data laws.

Concerning the DMA, the ex-ante nature of the regulation raised concerns according to Denmark, the Netherlands, and Slovakia. Moreover, the overlap with Article 102 TFEU was also noted by Czechia and Portugal as a source of concern. Germany, Netherlands, and Portugal mentioned issues with Articles 5 to 7 of the DMA.

	DSA	DMA
Austria	– Incorporation and horizontalization of the effects of Union fundamental rights in the relationship between the service provider and its users is unclear. – Transfer of far-reaching powers to certain actors, e.g., out-of-court dispute resolution bodies is questionable concerning the protection of fundamental rights. – The role of the Commission in the enforcement of the DSA was examined, especially in relation to other legal acts, e.g., DMA – The importance of clear tertiary legal requirements for independent review (Art. 37 DSA) was emphasized in the context that the DSA takes a self-regulatory approach. – The legal basis for claims for damages (Art. 54 DSA) is not harmonized and leads to a fragmentation of the internal market and the level of protection in actions for damages.	No issues yet.
Belgium	N/A	N/A
Bulgaria	Since the authorities to be designated to deal with the DSA/DMA have no experience, there is potential for many claims for state liability due to omission to act/take measures and lack of implementation on national level.	
Croatia	No issues yet.	No issues yet.
Czechia	– The Deputy Prime Minister for Digitalisation views the blocking measures to online services as a significant threat to the development of free digital markets. – Stakeholders seek clarity on how information sharing with law enforcement authorities will be managed.	– The Commission's process for selecting gatekeepers. – Prospects for a parallel private enforcement of the DMA and Article 102 TFEU.
Denmark	– Difficulty in locating mere conduit and caching services. – The DSA's use of delegated acts, e.g., for access for researchers to data, has led to a delay which is difficult to communicate to the persons affected. – Lack of a specific time limit for removal of illegal content has been criticized. – The interaction between the DSA and other acts, e.g., GDPR, is very complex	– The DMA being an ex-ante regulatory tool is an issue.

Finland	– The approach is not radical enough to reach the potential of the DSA and DMA – More active dissemination is required	
France	– There was a controversy surrounding the adoption of a Law on influencers and the provisions not in accordance with EU law were later removed. – The DGCCRF noticed that the economic actors on which diligence obligations are imposed are concerned with the lack of clarity of those obligations.	– The concept of cumulative legislation is unclear. – The legal nature of the ex-post aspect of the DMA is debated. – The possibility of implementing structural solutions is debated.
Germany	– There was criticism for the system of trusted flaggers and how it will play out in practice	– The ne bis in idem principle concerning the imposition of fines. – Concerning the duties of conduct, matters with cross-border implications. – The burden of presentation and proof in civil proceedings. – The manner with which German civil courts should deal with the categorical nature of Art. 5 to 7 DMA – To what extent proceedings in which courts have to ignore potentially valid objections to anti-competitive effects or justifications will lead to inequitable results.
Greece	No issues yet.	No issues yet.
Hungary	N/A	N/A
Italy	No issues yet.	No issues yet.
Latvia	No issues yet.	No issues yet.
Lithuania	– Google's proposal to limit the application of the DSA to the providers established in Lithuania was rejected and then accepted. – Internet media association has proposed to clarify that service providers only become aware of the infringing information is they receive credible data, which was accepted.	N/A
Netherlands	– Role of VLOPs and VLOSEs in the procedures is unclear.	– Risk of over-inclusiveness of the Regulation given its ex-ante nature. – Designation of gatekeepers – Art. 5 to 7 DMA have been discussed in terms of scope and enforceability.
Norway	No issues yet.	No issues yet.

Poland	– Role played by the supervisory authority for personal data – Proposal for regulation of orders in the amended Act on Providing Services by Electronic Means should be discussed – Legislative proposal for amendments of the civil procedure to enable claims against unknown defendants to facilitate lawsuits of online defamation.	
Portugal	– Art. 6(1)(a) DSA because the judgment of illegality implied in it was noted to foster conflicts – The possibility of the notice and action mechanisms being used to notify the platforms of breaches to their Terms and Conditions was discussed – The degree of diligence of an online platform when issuing an opinion on the illegality of the content under Art. 16(2) and Art. 14(4) DSA was discussed.	– Prohibitions of Art. 5 DMA are too inflexible as they do not demand corresponding proof of the harmful effects of a behaviour – The DMA imposes a one-size-fits-all approach to gatekeepers with considerably diverse business models – Ne bis in idem principle raises some concerns as the obligations of Art. 6 and 7 DMA seem to arise from court disputes in the context of Art. 102 TFEU – The DMA was criticized for having broad remedies while EU competition law imposes specific reparations rules – The possibility that access controllers not based in the EU will prefer to provide their services to less regulated territories – The possibility that only Big Tech companies will be able to afford compliance with the DMA
Romania	No issues yet.	N/A
Slovakia	Nothing specific.	– the relevance of legal basis of the DMA and its relationship with competition law, – claims for damages, private enforcement under DMA – applicability of competition-like efficiencies of EU-style rule of reason in the context of the ex ante regulation by the DMA.
Slovenia	The Ministry of Digital Transformation identified the following provisions as unclear: – Art. 22 (trusted flaggers) – Art. 40(4) (data access and scrutiny) – Art. 53 DSA (right to lodge a complaint) The Information Commissioner notes that Art. 26 and 28 overlap with the GDPR.	No issues yet.

Spain	N/A	– Implementation of the regulation at the national level might be problematic due to the lack of a clear reference to any rule relating to how private enforcement should work in practice – Risks might arise from the interactions between the Commission as the sole enforcer and the national application of competition law – Problems might arise from the potential overlap with the merger control regime
Sweden	N/A	– Private enforcement – Interplay between the DMA and the antitrust legal framework