Crowell

Client Alert

The Digital Services Act: EU Regulation of Intermediary Service Providers Imminent

July 7, 2022

On Tuesday, July 5th, the European Parliament adopted the Digital Services Act (DSA) with a resounding 539 votes in favor, 54 votes against and 30 abstentions. The DSA is but one part of the multifaceted European digital strategy and, together with the Digital Markets Act (DMA), makes up the Digital Services Package, initially proposed by the European Commission in December 2020 (see our previous alert of January 12, 2021). The DSA takes the form of a Regulation, directly applicable in all EU Member States, and will amend (but not fully replace) the 2000 e-Commerce Directive (Directive 2000/31/EC).

At the same time, the European Parliament also passed the DMA. Whereas the DMA aims at ensuring fair and contestable markets in the digital sector by imposing specific regulatory obligations on so-called "gatekeepers," i.e., major digital platforms with a powerful and entrenched position which act as important gateways for businesses to reach end users (see also our client alert of May 17, 2022), the DSA's primary aim is to make the online world a safer, more predictable and trusted environment for EU-based users. It does so by imposing due diligence obligations on online "intermediary services" (e.g., social media platforms and online market places), with the heaviest burdens falling on "very large online platforms" (i.e., those with at least 45 million monthly active users in the EU).

The DSA revamps the principle of the limitation of liability for online intermediaries contained in the e-Commerce Directive, but its core innovation is a new chapter on standards for transparency, and the accountability of all providers of "intermediary services" regarding illegal and harmful content.

This new Regulation is important for the broad category of providers of "intermediary services", which are subject to new obligations and heightened scrutiny, by new national authorities on the one hand, and by right holders (e.g., holders of intellectual property rights or image rights) and users on the other, since they may rely on new mechanisms to protect their rights.

In this alert, we will provide a high-level overview of the main principles and novelties in the DSA, without venturing into in-depth analyses of the new obligations and enforcement mechanisms at this stage.

Which online "intermediary services" fall within the scope of the DSA?

In the DSA's crosshairs are online "intermediary services" that transmit or store third-party content for EU-based users, spanning a broad range of activities in the digital sphere. This includes social media services, messaging services, cloud infrastructure services, content delivery networks, etc.

Importantly, the DSA will apply to intermediary services provided to users who have their place or residence or business in the EU, regardless of whether the providers of those services are based in the EU (similar to the approach in the General Data Protection Regulation (GDPR)).

Depending on the type of "intermediary services" provided, different regimes apply.

Adopting the same notions as the e-Commerce Directive, the DSA categorizes these intermediary services into different groups: **mere conduit services**, **caching services**, and **hosting services** (see our previous alert of January 12, 2021). These types serve to determine the applicable accountability regime.

Among the providers of hosting services, a distinction is made between "online platforms" and "very large online platforms," each subject to different levels of due diligence obligations:

- **Online platforms** are providers of hosting services which, at the request of a user, store and disseminate information to the public (unless that activity is a minor or a purely ancillary feature of another service or a functionality of the principal service and, for objective and technical reasons**,** cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the DSA). Examples include social media platforms and online market places.
- **Very large online platforms** are online platforms that, for at least four consecutive months, provide their services to at least 45 million average monthly active users in the EU (corresponding to approximately 10% of the EU population), and have been designated as such by the European Commission.

Specific rules are also introduced for "online search engines":

- **Online search engines** provide digital services that allow 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 (a definition borrowed from the 2019 Platform to Business Regulation).
- **Very large online search engines** are the search engines which reach, on average, at least 45 million monthly active recipients of the service in the EU, and have been designated as such by the European Commission.

This particular definition of "online search engines" sits uncomfortably with the scope of the Regulation, which explicitly and repeatedly states that the DSA applies to "intermediary services" (still to be distinguished from "intermediation services" in the Platform to Business Regulation). As "online search engines" are defined as "digital services" and do not seem to fit the definition of "intermediaries", the fairly late introduction of this definition creates confusion as to the application of the DSA to search engines.

While "very large" online platforms and search engines are subject to stricter due diligence obligations, there are exceptions for platforms that qualify as medium, or micro or small enterprises.

Core structure of the DSA

Definition of "illegal content"

The term "illegal content" is at the heart of the DSA. It is defined as any information or activity, including the sale of products or provision of services, which is not in compliance with EU law or the law of a Member State, irrespective of the precise subject matter or nature of that law. The DSA thus adopts a horizontal approach: its mechanisms apply to all kinds of illegal content (as diverse as hate speech, revenge porn, libel or infringement of intellectual property).

Liability of providers of intermediary services

The DSA regulates the exemptions from liability of providers of intermediary services, stating conditions under which providers of mere conduit services, caching services and hosting services may escape liability for illegal third-party information stored or transmitted by them. These new provisions in the DSA replace the preceding regime under the e-Commerce Directive (and its national transpositions).

As was the case under the e-Commerce Directive, there are no general monitoring or active fact-finding obligations for intermediary service providers. However, the DSA clarifies that intermediary service providers that diligently carry out voluntary own-initiative investigations in good faith or take measures aimed at detecting, identifying and removing, or disabling access to illegal content on their platforms are not per se disqualified from the exemptions.

By contrast, intermediary service providers are required to respond to orders of national judicial or administrative authorities to act against illegal content and provide information, while also maintaining a right to an effective remedy (such as the right to challenge an order).

Due diligence obligations for a transparent, accessible and safe online environment

The main novelty of the DSA resides in the obligations for the various types of intermediaries to ensure a safer, more accessible and more transparent online environment. The DSA uses a progressive system: the obligations become more onerous depending on the type of intermediary service provider.

At the least demanding level, **all intermediary service providers** will have to comply with certain obligations, both procedural (such as establishing points of contact for authorities and users and designating legal representatives in the EU for intermediary service providers established outside the EU) and substantive. The substantive obligations include ensuring that terms and conditions are fair, transparent and non-discriminatory, and setting out any restrictions that may be imposed on the use of their services. In addition, all intermediary service providers must comply with transparency reporting obligations and publish reports on content moderation and the removal of information considered to be illegal or non-compliant content.

Hosting service providers will additionally have to put "notice and action" mechanisms in place that allow users to notify the presence of alleged illegal content (with a sufficiently substantiated explanation why the

information is deemed illegal). The hosting provider can respond with different measures (restrictions, removal or termination) relating to the visibility of the content, the payment systems used, the provision of the service, or the user's account. Except in certain situations, the hosting service provider will have to provide the impacted user with a statement of reasons for the measure. Where a hosting service provider becomes aware of information giving rise to suspicions of serious criminal offences involving a threat to the life or safety of persons, it must promptly inform the competent enforcement authorities.

Further obligations will be imposed on **online platforms**. In their notice and action mechanism, they must create a role for "**trusted flaggers**" (a particular status awarded to independent entities upon meeting certain conditions) whose notices are to be treated with priority and processed without delay.

Providers of such services must set up an **internal complaints handling system** so that the user whose content was taken down as illegal or non-compliant can challenge this decision. Moreover, they must allow users to challenge such decisions before **out-of-court dispute settlement bodies** certified by the Digital Services Coordinators of the Member States (more about Digital Service Coordinators below).

Since online platforms play an important role in safeguarding the right to freedom of expression and other sometimes conflicting rights, they must also take measures against misuse of the platform, in particular against users who frequently provide manifestly illegal content or, conversely, frequently submit manifestly unfounded content.

With regard to **online marketplaces**, online platforms have a best effort obligation to assess the reliability of traders on their platforms. Moreover, taking the principle of compliance by design to the next level, the online platform must design their interfaces in such a way that traders comply with EU consumer and product safety law (this mainly regards information obligations). An online platform is obliged to intervene if it becomes aware that products and services traded using its platform are illegal: in that case, it must inform the consumers individually or by means of a public statement of this illegality and the means of redress.

Interestingly, the DSA regulates online platforms not only in their role as moderators of third-party content but also as an interface for the information they convey to users on their own account: the online interface of their platforms may not deceive or manipulate the users, they must control the presentation of advertising on their platforms and recommender systems, and they must protect minors.

Finally, **very large online platforms** will have to conduct extensive risk assessments on the "systemic risks" brought about by or relating to the design, algorithmic systems, intrinsic characteristics, functioning and use of their services and take reasonable and effective risk mitigation measures. Systemic risks include, in addition to the "dissemination of illegal content", negative effects on fundamental rights (human dignity, privacy, personal data, freedom of expression), on civic discourse and electoral processes or public security, gender-based violence, minors, public health and the physical or mental well-being. The DSA is thus intended to address complex problems such as mass disinformation and its impact on democratic processes or public health, and the systematic trolling and marginalization of communities.

The DSA also establishes a **crisis response mechanism**, allowing the European Commission to require very large online platforms to take certain actions to investigate and respond to serious threats to public security or health in the EU.

In order to monitor compliance with these obligations, very large online platforms have to undergo external and **independent audits** – and this may raise important questions relating to the protection of the platforms' intellectual property and trade secrets. Upon request, very large online platforms will also have to grant Digital Service Coordinators (see below) access to data in order to monitor their compliance with the DSA. Such platforms must also establish independent compliance officers, who will monitor compliance with the DSA and must have access to the platform's management body.

Implementation and enforcement of the DSA

The DSA has its own enforcement system (similar to the enforcement mechanisms in the GDPR), in which the **Digital Service Coordinators** (DSCs) will play a crucial role. The Member States are required to designate DSCs, which will act as the national authorities supervising the providers of intermediary services and their compliance with the DSA. DSCs will deal with complaints against intermediary service providers regarding breaches of the DSA, and will have powers of investigation and enforcement (remedies and sanctions). Coordination and consistency across DSCs is ensured through specific mechanisms (such as mutual assistance or cross-border cooperation among DSCs). In addition, the DSA will create the **European Board for Digital Services**, an independent advisory group for the DSCs.

Specific enforcement systems are put in place for the very large online platforms and very large online search engines, giving the **European Commission** extensive powers to intervene vis-à-vis platforms that persistently infringe. The DSA bestows upon the Commission considerable investigatory powers, which it may even exercise on its own initiative and before initiating proceedings. In case of non-compliance, the Commission can impose periodic penalty payments and impressive fines (up to 6% of the global turnover), as well as employ an enhanced supervision system to monitor how very large online platforms or search engines remedy infringements of the DSA. Very large online platforms and search engines will of course have a right to be heard and must be granted access to the file in case of non-compliance measures taken by the Commission. The Court of Justice of the European Union has unlimited jurisdiction to review the Commission's decisions.

What's next?

Following its adoption at first reading by the European Parliament, the DSA must now be formally adopted by the Council of the European Union. After signature, the DSA will be published in the Official Journal and will enter into force 20 days after its publication, probably in the autumn of 2022. The DSA will apply either 15 months after its entry into force or from 12 January 2024, whichever is later. The specific obligations for very large online platforms will apply four months after their designation as such by the Commission.

Commissioner Breton has already announced that, in order to ensure the enforcement of the DSA and the DMA, dedicated teams within DG Connect will be organized around thematic domains, handling the societal (such as risk assessment and audits), technical (covering issues such as interoperability) and economic (examining unfair

trading practices or liability exemptions) issues. These dedicated teams will be coordinated by a "program office" also dealing with international issues and litigation. The 100+ full time staff of DG Connect will comprise all the required expertise (including in data science and algorithms) and supposedly be financed using the fees that the Commission will collect from the very large online platforms and search engines.

The authors thank Ms Florence Nieuwbourg for her assistance in preparing this alert.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Sari Depreeuw
Partner – Brussels
Phone: +32.2.282.18.49
Email: sdepreeuw@crowell.com

Karl Stas
Senior Counsel – Brussels
Phone: +32.2.214.2888
Email: kstas@crowell.com

Sander Vogt
Associate – Brussels
Phone: +32.2.214.2812
Email: svogt@crowell.com