TechSpeak Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Digital Services Act: Protecting the Digital Space Against the Spread of Illegal Content

July 20, 2022

Key Points

- The European Parliament has reached agreement on new legislation to require certain providers of online services to comply with new obligations in order to ensure online safety and to prevent the spread of illegal content.
- The legislation has not yet fully passed through the EU's legislative process, but at this stage the text is in a state that allows businesses to consider the impact of the additional obligations on their operations.
- The legislation applies to all online intermediaries – whether they are established inside or outside the EU – which are offering services to people/entities within the EU.
- The practical effects of the legislation will likely include increased compliance costs for businesses, possible organisational/personnel changes at a compliance level and increased accountability to relevant authorities.
- The maximum fine for breach will be 6% of global annual turnover in the preceding financial year.
- The new legislation is in the form of a Regulation, which is directly applicable in all 27 EU Member States. The UK, now outside of the EU, has its own new legislation in this area in the form of the Online Safety Act.

Introduction

The European Parliament has reached agreement on a text of the Digital Services Act (DSA)[1]. The DSA is designed to regulate the conduct of providers of so-called "intermediary services", i.e. those which connect consumers and/or users to goods, services or content online. The DSA will, notably, govern the conduct of online search engines and online platforms, such as social media and marketplaces.

As noted below (see "Next Steps" below), the DSA has not yet passed fully through the legislative process of the European Union (EU). However, we expect that it is in near-final form, with only a handful of particular provisions still likely to be subject to further discussion, if any.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Davina Garrod
Partner
Davina.garrod@akingump.com
London
+44 20.7661.5480

Jenny Arlington
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

Mark Gleeson
Counsel
mark.gleeson@akingump.com
London
+44 20.7661.5461

Alexander Armytage
Associate
Alexander.armytage@akingump.com
London
+44 20/7012.9651

We set out below the headline points that businesses should be aware of when the DSA comes into effect.

Background

The EU has recognised the need to update its legislation on information society services, in particular intermediary services, as an important part of the life of Union citizens and the EU's economy. The DSA is, in effect, a replacement for the EU's last legislation in this space, which was adopted in 2000. Since then, innovative business models that have developed online have presented new opportunities and risks for EU citizens, prompting the need for updated regulation.

The aim of the new legislation is to protect the digital space against the spread of "illegal content" and at the same time ensure the protection of users' fundamental rights. The definition of "illegal content" is broad and includes any information which, in itself or in relation to an activity, is not in compliance with EU or Member States' laws, irrespective of the subject matter of such laws.

Territorial Scope

The DSA will apply to all online intermediaries offering services both to natural people resident in the EU and/or legal entities established or located in the EU, regardless of the intermediary's place of establishment or location.

An online intermediary will be "offering services" if it is enabling natural or legal persons to use the services of a provider which has a "substantial connection" to the EU. The assessment of a "substantial connection" will be based on factual criteria, such as a significant number of recipients of the service in one or more Member States in relation to its or their population, the targeting of activities towards one or more Member States, or an establishment in the EU.

Range of Providers Caught

The DSA will impose different obligations on four categories of intermediaries. The four categories are:

I. All intermediary services: providers of one of any of three services: (i) "mere conduit", i.e. transmission of information in, or providing access to, a communication network (e.g. internet exchange points); (ii) "caching", i.e. transmission of information together with automatic/ temporary storage (e.g. reverse proxies); and (iii) "hosting", i.e. storage of information (e.g. web hosting).

II. Hosting services: as described above (e.g. cloud and web hosting services, and social media), where the service disseminates information to the public as a main feature (services that disseminate as a minor functionality are not captured).

III. Providers of online platforms: providers of hosting services which, at the request of a recipient of the service, store and disseminate information to the public, unless those activities are a minor and purely ancillary feature of the principal service (e.g. online marketplaces, app stores, social media).

IV. Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs): online platforms which provide their services to a number of average monthly active service recipients in the EU equal to or higher than 45 million.

The first (and largest) category encompasses all providers of intermediary services, and they will be subject to a threshold level of new obligations. Each subsequent category encompasses a progressively narrower set of intermediaries, who will be subject to a progressively more onerous set of new obligations. Thus, each subsequent category has to comply with the obligations imposed on the previous categories, as well as additional obligations. The narrowest group, subject to the most (and most stringent) requirements, is that of VLOPs and VLOSEs. Providers designated as VLOPs/VLOSEs, i.e. Category 4, will therefore have to comply with the obligations applicable to all four categories.

Key Obligations

Below we set out some of the key obligations.

1. *All intermediaries (categories 1-4)*
    a. Transparency, including the provision of specified information in terms and conditions and the publication of annual reports (or more frequently for VLOPs).
    b. Compliance with orders to provide information or to act against illegal conduct.
    c. Designation of a point of contact and, for intermediaries not established in the EU but offering services in the EU, a legal representative.
    d. Limitation of liability in certain circumstances.
2. *Hosting services (Categories 2-4)*
    a. "Notice-and-action" mechanism to allow any individual or entity to notify them of illegal content (the "notice" mechanism) and to process any notices and take decisions. Notices submitted by "trusted flaggers" (see below) have to be treated with priority.
    b. Reasons for decisions: When a provider decides to remove or disable access to specific information provided by a service recipient, it must inform the affected recipient(s) of the decision and publish it on a public database.
    c. Notification of suspicions of criminal offences: A hosting provider must inform the relevant law enforcement authorities as soon as it becomes aware of information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place.
3. *Online platforms (Categories 3-4)*
    a. Illegal content and abusive notices: After having submitted a warning, online platforms must suspend their services to recipients that frequently provide manifestly illegal content. Online platforms must also suspend the processing of notices and complaints submitted by persons that frequently submit notices or complaints that are manifestly unfounded.
    b. Trusted flaggers: Online platforms must process with priority notices on illegal content submitted by trusted flaggers, who are designated by Digital Service Coordinators.
    c. Complaint handling system: Online platforms must maintain an internal, user-friendly, easily accessible electronic complaint management system, which

recipients must have access to for submitting complaints electronically against the online platform's decisions on illegal content.

d. Out of court dispute settlement: Recipients affected by an online platform's decision on illegal content are entitled to turn to an out-of-court body certified by the Digital Services Coordinator (see "Enforcement" below). Online platforms are bound by the decision of this body.

e. Enhanced transparency, including in the annual reports: Online platforms must disclose information in their annual reports about out-of-court disputes, suspensions imposed on recipients and automated content moderation. They must also publish, at least once every six months, information on the average monthly active recipients of their service.

f. Advertising transparency: Online platforms must ensure that the recipient of the service can identify, for each specific advertisement, that the information displayed is an advertisement, on whose behalf the advertisement is and meaningful information about the parameters used to determine the recipient of the advertisement.

g. Recommender system transparency: If an online platform uses a recommender system, it must provide certain information about this in its terms and conditions.

h. Online protection of minors: Where an online platform is accessible to minors, it must put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security in respect of minors.

i. Traceability of traders: When an online platform allows consumers to conclude distance contracts with traders, it must identify the traders and obtain certain information (listed in the DSA) about them before allowing them to use the platform's services.

j. Reporting suspected criminal offences: If an online platform becomes aware of any information which gives rise to a suspicion that a criminal offence involving a threat to the life or safety of persons is taking place, it must promptly inform the local competent law enforcement authorities.

k. Exclusion for micro and small enterprises: The obligations on online platforms do not apply to online platforms that qualify as micro or small enterprises.

4. VLOPs and VLOSEs (Category 4)

a. Risk assessment: VLOPs must identify, analyse and assess the significant systemic risks stemming from the functioning and use of their services in the EU and must put in place reasonable, proportionate and effective risk-mitigation measures.

b. Crisis response mechanism: Where a crisis occurs, the European Commission may require VLOPs and VLOSEs to adopt certain steps to reduce the risk, threat or impact of such crisis.

c. Independent audits: VLOPs and VLOSEs must conduct annual audits, at their own expense, on compliance with the DSA by an independent external auditor. The auditor must issue a written report and, where the audit is "positive with

comments" or "negative," include operational recommendations on specific measures to achieve compliance.

d. Further transparency requirements for recommender systems and online advertising: VLOPs and VLOSEs that use a recommender system must make the main parameters used by such systems clear and accessible in their terms and conditions. Those that display advertising on their online interfaces must make public, through an anonymised repository, the content of the advertisement, on whose behalf the advertisement is, the period during which the advertisement was displayed and certain information about the target audience of each advertisement. VLOPs and VLOSEs must also publish the transparency reports every six months (rather than annually), as well as publish annually other reports in relation to their obligations.

e. Data sharing: VLOPs and VLOSEs must provide access, upon request, to data for monitoring and assessing compliance to the Digital Services Coordinator or the European Commission, and must grant access to the data to vetted independent researchers that will work to identify and understand any systemic risks.

f. Compliance function: Each VLOP must establish a compliance function, which is independent from operational functions, consisting of at least one professional compliance officer to monitor compliance with the DSA. The head of the compliance function must be an independent senior manager with appropriate professional qualifications, knowledge, experience and ability, whose responsibilities are distinct from the operational functions. The compliance officer's name and contact details must be provided to the Digital Services Coordinator and the European Commission.

g. Terms and conditions (languages): VLOPs and VLOSEs must publish their terms and conditions in the official languages of all Member States in which they offer their services.

Enforcement

The maximum fine for breach of the DSA will be 6% of global annual turnover in the preceding financial year.

Supervision and enforcement will generally be carried out by national regulatory authorities described as "Digital Services Coordinators." The Digital Services Coordinators will have the power to order the cessation of alleged infringements of the DSA, adopt interim measures to avoid the risk of serious harm and impose remedies, fines and periodic penalty payments.

The European Commission will have exclusive power to supervise the obligations of VLOPs and VLOSEs to manage systemic risks under the DSA.

At the EU level, there will be a European Board for Digital Services: an independent advisory group which will support the European Commission, help coordinate the actions of Digital Services Coordinators and contribute to the drafting of templates and codes of conduct as envisaged under the DSA.

Next Steps

The DSA is being adopted via the EU's ordinary legislative procedure, whereby the Council and Parliament both need to agree on the legislative text initially proposed by the Commission. On 5 July, Parliament adopted the DSA at the first reading by an overwhelming majority. The Council can now decide whether to accept Parliament's position, in which case the legislation is fully adopted, or it may introduce its own edits and trigger a second reading by Parliament. If the Council does not accept all the amendments adopted by Parliament at the second reading, a conciliation procedure is initiated with the aim of agreeing on a joint text that harmonises the positions of Parliament and the Council.

Considering Parliament's overwhelming support for the current draft, as well as the fact that on 23 March 2022 Parliament and the Council had reached a provisional political agreement on the DSA, the Council is not expected to introduce significant amendments when it votes on the text in September. However, the possibility that Member States will push for their own version of the text should not be ruled out. In that case, the adoption process of the DSA could be drawn out for several more months.

If the Council adopts the text in September, the DSA will enter into force 20 days following its publication in the *Official Journal of the European Union*. It will be directly applicable across the EU 15 months after its entry into force, or on 1 January 2024, whichever is later. However, VLOPs and VLOSEs will be subject to the obligations in the DSA four months after they have been designated as such by the Commission, even if such date is earlier than 15 months after entry into force or 1 January 2024.

Conclusions

The DSA will impose additional obligations on many businesses that operate in the online information space in the EU. Businesses will first need to consider what category they fall under, and then the obligations imposed on them according to that categorisation.

Until the DSA is passed by the Council and put into effect, businesses should start to consider these questions well in advance in order to equip themselves for full compliance.

[1] Officially, the DSA is the Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 200/31/EC.

akingump.com