YOU MAY BE SUBJECT AS WELL!: DIGITAL SERVICES ACT – WHAT COMPANIES NEED TO KNOW

BY
JULIA APOSTLE

&
KELLY HAGEDORN

&
CHRISTIAN SCHRODER

&
ADELE HARRISON

Julia Apostle, Partner at Orrick Paris; Kelly Hagedorn, Partner at Orrick London; Christian Schröder, Partner at Orrick Germany & Adele Harrison, Managing Associate at Orrick London.

Visit www.competitionpolicyinternational.com for access to these articles and more!

YOU MAY BE SUBJECT AS WELL!: DIGITAL SERVICES ACT – WHAT COMPANIES NEED TO KNOW

By Julia Apostle, Kelly Hagedorn, Christian Schroder & Adele Harrison

The EU Digital Services Act ("DSA") is in force and the first of its requirements will soon take effect. And yet, many businesses do not even know yet that they are subject to the DSA. The landmark legislation DSA has a large scope of application, covering a significant range of online services that target EU users. In particular, companies that make available to the public any third-party content, whether B2B or individual user content, may be subject to its rules. This article provides an overview of the DSA, including its scope of application, key obligations and when these take effect, and sanctions for violations. It will also identify some of the steps that organisations should be taking now to achieve compliance.

01

WHY SHOULD COMPANIES BE READING THIS?

Even though the new EU's Digital Services Act ("DSA")[2] will impose many new compliance and reporting requirements for many businesses, most businesses have not yet started preparing as they may consider the DSA to only apply to the Big Tech companies. This is a misunderstanding. The DSA applies to many more companies than just Big Tech. By February 2023, companies will need to demonstrate compliance with initial notification requirements.

This article provides a brief overview on "who should comply" with the DSA and we will summarize the main requirements.

02

WHO MUST COMPLY WITH THE DSA? JURISDICTION AND KEY DEFINITIONS

The DSA applies to "intermediary services offered to "recipients of the service" that have their place of establishment or are located in the EU. The location of establishment of the intermediary service outside of the EU will not prevent application of the law.

An "intermediary service" basically covers all companies which show/process third party content on their website. Even a mere "comment function" on a website allowing third parties to share their views may trigger the application of the DSA.

More specifically, the DSA defines "intermediary service" as a "mere conduit" service, "caching" services, "hosting" services and "online search engines." Hosting services are further divided into "online platforms" and "very large online platforms" ("VLOPs"). There is also a sub-category of "very large online search engine" ("VLOSE").

A "recipient of the service" is defined as a "natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible."

The nature and scope of the obligations applicable to an intermediary service depend on the classification of the intermediary service provider into one of these categories. Therefore it will be important to assess whether an online service provider qualifies as an intermediary and, if so, which category of intermediary. At one end of the spectrum, with most obligations, are VLOPs and VLOSEs. At the other end, with the least number of requirements with which to comply, are "mere conduits" and "caching" services. The categories are defined by the DSA as follows:

- A "**mere conduit**" transmits information provided by a recipient of the service in a communication network, or provides the access to a communication network (examples include VPNs, wireless access point, internet exchange points, top-level domain name registries).
- A "**caching**" service involves the automatic, intermediate, and temporary storage of information transmitted in a communication network of information provided by a recipient of the service (examples include database caching, web caching).
- A "**host**" stores information provided by and at the request of a recipient of the service (examples include cloud storage services, online platforms).
- An "**online platform**" is a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public (examples include online marketplaces, social networks, collaborative economy platforms). If the storage and dissemination functionality is only a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, then it will not be considered as an online platform but may still qualify as a host.
- An "**online search engine**" is a digital service that allows users to input queries in order to perform searches of a website or all websites, in a particular language in the form of a keyword, voice request, phrase or other input, and return results in any format (examples include Google search, Bing, Brave, and others).

The decision to designate an online platform as a VLOP or VLOSE is made by the European Commission, provided the platform has a number of average monthly recipients of the service that is higher than 45 million. The definition of an "active recipient of an online service" is not necessarily

2 Formal title: 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.

the same as an "monthly active user," which is a common measure of site engagement. Under the DSA, an active recipient is a "recipient of the service that has engaged with an online platform, either by requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface."

03

WHEN DOES THE DSA TAKE EFFECT ?

The obligations of the DSA come into effect in a staggered manner. The very first obligation must be complied with by **February 17, 2023,** which is just around the corner. Article 24(3) of the regulation requires online platforms and online search engines to publish, on their website, starting February 17, 2023 and at least every 6 months thereafter, the number of average active monthly recipients of the service.

Most of the other obligations come into force by February 17, 2024, except that the VLOPs and the VLOSEs are subject to a much shorter compliance timeframe.

04

NATURE OF THE OBLIGATIONS

As already noted, the application of obligations depends on the nature of intermediary service, and even the minimal requirements may be considerable for individuals businesses.

All intermediary service providers will be required to do the following:

i. Act against items of illegal content (e.g. take them down) and/or provide the requested information about individual service recipients upon receipt of a duly issued order by the relevant national authority (the DSA specifies the conditions to be satisfied by such orders). The concept of "illegal content" is defined as "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." Thus, the application and interpretation will vary from Member State to Member State and may thus require significant resources on the company's side when determining what content is illegal and in which jurisdiction.
ii. Identify a single point of contact within the organization who will be the point of contact for liaison with national authorities. Intermediaries that do not have an establishment in the EU will have to appoint a legal representative in a Member State where the intermediary offers its services (there may be a possibility of collective representation for micro, small, and medium enterprises). Since, however, the representative will be liable for actions of the represented company, it may not be easy to find such representatives.
iii. Comply with specific obligations in relation to the form and content of the intermediary service terms and conditions. For instance, the terms must be fair, non-discriminatory, and transparent, and must include information regarding how to terminate services, restrictions imposed on the delivery of services, and also regarding the use of algorithmic tools for content-moderation. Details of rules of internal complaints handling systems should also be disclosed.
iv. For services provided to minors or pre-dominantly used by them, the terms must be expressed in easily understandable language.
v. Protect the anonymity of users except in relation to traders.
vi. Publish an annual transparency report on any content moderation then engaged in, including specified information such as the number of orders received from Member States' authorities, response times, and information about the own-initiative content moderation practices of the service, including the use of automated tools and the restrictions applied, and information about the training and assistance provided to moderators. (This obligation does not apply to micro or small enterprises that do not qualify as very large online platforms). These obligations, and others, will require the implementation of specific internal processes in order to capture the required information.

Additional obligations for hosting services, including online platforms include the following:

i. Hosting services must have a notification mechanism allowing the signalling of content considered by a user to be illegal content. The mechanism must be designed to facilitate sufficiently precise and substantiated notices to permit the identification of the reported content.
ii. Hosting services must provide a statement of reasons to the user if their content is disabled or removed or if services are suspended. This explanation must

contain certain information, including the facts relied upon and a reference to the legal ground relied upon, or other basis for the decision if it was based on the host's terms and conditions. However, law enforcement authorities may request that no explanation is provided to users.

iii. There is a positive obligation to alert law enforcement or judicial authorities if the host suspects that a serious criminal offence involving a threat to life or safety of persons is taking place or is planned.

iv. The anonymity of the content reporter is to be protected, except in relation to reports involving alleged violation of image rights and intellectual property rights.

v. The transparency reports prepared by hosting services will have additional information, including the number of reports submitted by trusted flaggers and should be organized by type of illegal content concerned, specifying the action taken, the number processed by automated means and the median response time.

> ***The application of obligations depends on the nature of intermediary service, and even the minimal requirements may be considerable for individuals businesses***

The additional obligations for online platforms include the following. The obligations in this section do not apply to micro or small enterprises, except if they qualify as very large online platforms. Intermediary services may apply to be exempted from the requirements of this section of the DSA.

i. Online platforms must provide an appeal process against decisions taken by the platform in relation to content that is judged to be illegal or in breach of the platform's terms and conditions. The relevant user will have six months to appeal the decision. Decisions must not be fully automated and must be taken by qualified staff.

ii. Users will be able to refer decisions to an out-of-court dispute settlement body certified by the Digital Services Coordinator of the relevant Member State. Clear information regarding this right must be provided on the service's interface.

iii. Content reported by trusted flaggers must be processed with priority and without delay. An entity may apply to the Digital Services Coordinator to be designated as a trusted flagger, based on criteria set out in the DSA.

iv. The suspension of users, for a reasonable period of time, is permitted if they repeatedly upload illegal content, after issuing a prior warning. Online platforms must also suspend the processing of notices and complaints from users that repeatedly submit unfounded notices and complaints.

v. Online platforms are required to ensure that their services meet the accessibility requirements set out in the EU Directive 2019/882, including accessibility for persons with disabilities, and must explain how the services meet these requirements.

vi. There is a specific prohibition applicable to online platforms in relation to the use of "dark patterns." The European Commission may issue further guidance in relation to specific design practices. The prohibition does not apply to practices covered by the Directive concerning unfair business-to-consumer practices, or by the GDPR.

vii. To ensure the traceability of traders (i.e. professionals that use online platforms to conduct their business activities), online marketplaces must only allow traders to use their platform if the trader first provides certain mandatory information to the platform, including contact details, an identification document, bank account details, and details regarding the products that will be offered. Online platforms must make best efforts to obtain such information from traders that are already using the platform services within 12 months of the date of coming into force of the DSA.

viii. A trader who has been suspended by an online platform may appeal the decision using the online platform's complaint handling mechanism.

ix. Online platforms that allow consumers to conclude distance contracts with traders through their services must design their interface so as to enable traders to provide consumers with the required pre-contractual information, compliance and product safety information. Traders should be able to provide clear and unambiguous identification of their products and services, any sign identifying the trader (e.g. a logo or trademark), and information concerning mandatory labelling requirements.

x. Online platforms must make reasonable efforts randomly to check whether the goods and services offered through their service have been identified as being illegal. If an online platform becomes aware that an illegal product or service has been offered to consumers it must, where it has relevant contact details or otherwise by online notice, inform consumers of the illegality and the identity of the trader, and available remedies.

xi. To promote online advertising transparency, online platforms must ensure that service users receive the following information regarding online ads: that the content presented to users is an advertisement, the identity of the advertiser or person that has financed the advertisement, information regarding the parameters used to display the ad to the user (and information about how a user can change those parameters).

xii. Targeting techniques that involve the personal data of minors or sensitive personal data (as defined under the GDPR) is prohibited.
xiii. Online platform providers must provide users with functionality that allows them to declare that their content is a "commercial communication" (i.e. an advertisement / sponsored content).
xiv. Online platforms have transparency obligations regarding any recommender system that is used to promote content. The online platform must disclose the main parameters used, as well as options for the recipient to modify or influence the parameters.

Additional obligations for VLOPs and VLOSEs include the following:

i. VLOPs and VLOSEs must publish their terms and conditions in the official languages of all Member States where their services are offered (this is often a requirement of national consumer protection law as well).
ii. VLOPs and VLOSEs must carry out (and in any event before launching a new service), an annual risk assessment of their services. The risk assessment must take into account in particular risks of dissemination of illegal content; negative effects for the exercise of the fundamental rights; actual or foreseeable negative effects on civic discourse and electoral processes and public security; in relation to gender-based violence; public health; minors; and physical and mental well-being. VLOPs and VLOSEs must consult with user representatives, independent experts and civil society organizations.
iii. VLOPs and VLOSEs must implement mitigation measures to deal with these systematic risks. The DSA lists measures that might be adopted.
iv. VLOPs and VLOSEs must have independent audits carried out at least once a year, by independent firms, to assess their compliance with the DSA requirements and any commitments undertaken pursuant to a code of conduct. The DSA imposes certain conditions on the firms that must conduct such audits (e.g. they must be independent and free of conflicts of interest).
v. VLOPs and VLOSEs may be required by the Commission to take certain specified actions in case of a crisis, including conducting an assessment to determine whether the service is contributing to the serious threat and to adopt measures to limit, prevent or eliminate such contribution.
vi. VLOPs that use recommender systems must provide at least one that is not based on profiling and must provide users with functionality to allow them to set their preferred options for content ranking.
vii. Additional advertising transparency obligations are applicable, requiring the publication of information regarding the advertisements that have been displayed on the platform, including whether the advertisement was targeted to a group, the relevant parameters and the total number of recipients reached. The information should be available through a searchable tool that allows multicriteria queries.
viii. VLOPs and VLOSEs are required to share data with authorities, where necessary for them to monitor and assess compliance with the DSA. Such information might include explanations of the functioning of the VLOPs algorithms. The regulator may also require that VLOPs allow "vetted researchers" (those that satisfy the DSA's requirements) to access data, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks.
ix. VLOPs and VLOSEs must appoint a compliance officer responsible for monitoring their compliance with the DSA.
x. VLOPs and VLOSEs must pay the Commission an annual supervisory fee to cover the estimated costs of the Commission (the amount is still to be determined).

05

OTHER KEY ELEMENTS OF THE DSA

A. Intermediary Liability

The DSA retains the exemption contained in the eCommerce Directive, which provides that intermediaries are not liable for information transmitted through their services, provided they were not actively involved in the transmission and/or they acted to remove or disable access to the information upon receiving notice. There is a modification to this exemption with the DSA, in that it imposes on hosts (and the subset categories of online platforms and very large online platforms) a set of due diligence requirements in relation to illegal content, as described above in relation to specific obligations. In addition, the text retains the principle that intermediaries will not be subject to a general monitoring obligation, however as stated in Recital 30, "this does not concern monitoring obligations in a specific case."

B. Interaction With Other Laws

Importantly, the DSA does not override existing EU and national legislation and therefore there will be areas of overlap among the DSA obligations and those set out in other laws. For instance, both the DSA and the EU Platform to Business Regulation 2019/1150 contain transparency and operational requirements in relation to the use of recommender

systems. The Online Terrorist Content Regulation 2021/784 also contains specific notice and action obligations in relation to terrorist content, and both the Audiovisual Media Services Directive 2010/13/EU and the EU Copyright Directive 2019/790, as implemented nationally, cover some of the same ground. Since compliance with some of the DSA requirements will be facilitated by the use of AI technology, the EU's AI Act, which is currently close to adoption, will also need to be taken into consideration. And of course, the various EU Member States have their own laws applicable to illegal content – not to mention differing standards as to what constitutes illegal content.

In practical terms, this means that companies subject to the DSA should not only be identifying the obligations in that law with which they must comply, but also how their DSA obligations intersect with other applicable legal requirements. Companies should also take note of the different national enforcement authorities that may have competence in relation to the overlapping legal obligations. In France, for instance, it is the consumer rights authority ("DGCCRF") that is responsible for enforcing the Platform to Business Regulation, but it will likely be Arcom that is the Digital Services Coordinator (see the section on Enforcement, below). National data protection authorities will also have a role, given that certain of the DSA provisions deal with the processing of personal data (see below).

C. Impact for the Online Advertising Ecosystem

The transparency obligations imposed on online platforms in relation to the advertising on their sites will most certainly result in the contractual flow-through of DSA obligations to participants in the online advertising ecosystem that are not directly subject to the regulation. For example, the obligation to ensure that online ads are appropriately identified as such, and that users are informed of the identity of the advertiser and of applicable targeting parameters, may require cooperation of ad tech providers. In addition, the prohibition against ad targeting based profiling, as defined by the GDPR, using sensitive personal data, will also pose technical compliance problems, especially in light of European Court of Justice's recent case law that adopts a very broad approach to the definition of special category data, specifically including indirectly inferred information.[3]

06
SANCTIONS & ENFORCEMENT

A. Sanctions

Temporary access restrictions. Where enforcement measures are exhausted, and in the case of persistent and serious harm, the Digital Services Coordinator may request that the competent judicial authority of the Member State order the temporary restriction of access to the infringing service or to the relevant online interface.

Fines. Sanctions must be "effective, proportionate and dissuasive." Member States must ensure that the maximum number of penalties imposed for a failure to comply with the provisions of the DSA must be 6 percent of the annual worldwide turnover of the intermediary or other person concerned. The maximum amount of a periodic penalty payment must not exceed 5 percent of the average daily turnover of the provider in the preceding financial year per day.

B. Enforcement

Each Member State must designate one or more competent authorities as responsible for the application and enforcement of the DSA, and one of these authorities must be appointed by the Member State as its Digital Services Coordinator. Except for the VLOPs and the VLOSEs, this Digital Services Coordinator will be the main enforcement authority. For non-EU based intermediaries, the competent Digital Services Coordinator will be located in the Member State where these intermediaries have appointed their legal representative. If no legal representative has been designated, then all Digital Services Coordinators will be competent to act. The European Commission will have exclusive jurisdiction in relation to enforcement of the obligations specifically applicable to the VLOPs and VLOSEs, and may assume jurisdiction to enforce other obligations against the VLOPs and the VLOSEs.

Digital Services Coordinators are granted investigation and enforcement powers — including the power to accept intermediary services' commitments to comply with the DSA, order cessation of infringements, impose remedies, fines, and periodic penalty payments.

A recipient of the service has the right to lodge a complaint against providers of intermediary services alleging an infringement of the DSA with the Digital Services Coordinator of the Member State where the recipient resides or is established.

3 See https://curia.europa.eu/juris/document/document.jsf;jsessionid=5CBD746EB4FD0D8B4D0DC7461B5B0129?text=&docid=263721&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8887343.

07
WHERE TO START

Companies with an online presence should already be determining whether they are subject to the terms of the DSA by virtue of qualifying as an online intermediary. If so, does the company offer its services in Europe and does it have an establishment in Europe? It may be necessary to identify and appoint a potential legal representative.

In parallel, following classification into a category of intermediary, it will be necessary to identify the applicable obligations, and the different teams or individuals within the company who will be part of implementing a compliance strategy. Cross-functional collaboration from the outset will be essential.

And do not forget the reporting obligation from February 2023.

Companies with an online presence should already be determining whether they are subject to the terms of the DSA by virtue of qualifying as an online intermediary

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL