The Digital Services Act (DSA) Transforms Regulation of Online Intermediaries

July 19, 2022

On July 5, 2022, the European Parliament voted to approve the final text of the Digital Services Act ("DSA" or the "Act"), a landmark regulation that—along with its sister regulation, the Digital Markets Act ("DMA")—is poised to transform the global regulatory landscape for social media platforms, hosting services like cloud service providers, and other online intermediaries.

Lawmakers have billed the DSA as implementing the principle that "what is illegal offline, should be illegal online." In reality, the DSA goes much further, requiring online platforms to not only take greater accountability for "illegal" and "harmful" content that they host, but also to provide unprecedented transparency around their content moderation practices, targeted advertising, and recommender algorithms, and to maintain comprehensive risk management systems for a potentially wide range of systemic risks—from public health crises to political misinformation.

In this Debevoise Data Blog post, we have provided an update on the status of the DSA, an overview of the key features of this landmark regulation, and several take-aways for companies about the import of the DSA.

Status of the DSA

The Parliamentary vote was the penultimate step for enactment of the DSA, which is now due to be adopted by the European Council in September 2022, formally enacting it as law. The Act was first introduced in December 2020, but stalled for negotiations between the European Council and Parliament. A political agreement was reached in late April 2022, and the text of the Act was finalized in the subsequent months leading up to the July Parliamentary vote.

Once adopted, the timeline for its application and enforcement will be fast-paced. While the full text of the DSA would begin applying to all covered online intermediary services on January 1, 2024, companies designated as very large online platforms ("VLOPs") may

have to begin complying with a subset of provisions at a much earlier date, most likely in early or mid-2023.

Scope of the DSA

The DSA applies to a wide range of "intermediary services," which the Act categorizes by the role, size, and impact of a given company on the online ecosystem. "Intermediary services" include a broad range of "mere conduit," "caching," and "hosting" services, with the bulk of the Act's requirements focused on the following types of companies:

- **Hosting services** that store information provided by, and at the request of, the user, such as certain cloud computing and web hosting services;
- **Online platforms** that are hosting services that store and disseminate information to the public (such as social networks), or that bring together sellers and consumers (such as online marketplaces and app stores);
- **Very large online platforms** ("VLOPs") that provide their services to over 45 million average monthly active recipients in the EU;
- **Online search engines** that allow users to input queries in order to perform searches and return results; and
- **Very large online search engines** ("VLOSEs") serving more than 10% of the 450 million consumers in the EU.

Under the Act, VLOPs and VLOSEs are subject to the most stringent set of requirements, as well as greater regulatory oversight.

Key Provisions for Platforms and Services

The DSA imposes tiered requirements on different categories of intermediary services, which means that a different set of obligations will apply to each type of intermediary covered under the Act. However, the general requirements of the Act are as follows:

Prohibitions

The DSA imposes outright bans on the following practices for all providers of online platforms:

- The use of *dark patterns* (i.e., confusing or deceptive user interfaces designed to steer users into making certain choices) (Art. 23a).
- Targeted advertising techniques that process, reveal, or infer *personal data about minors* for the purpose of displaying advertisements (Art. 24b).
- Targeted advertising directed at individuals on the basis of *certain sensitive categories of personal data* (as defined by GDPR Art. 9(1)), such as religion, sexual orientation, or ethnicity (Art. 24(3)).

Accountability for "Illegal" and "Harmful" Content

The DSA increases intermediaries' obligations to counter illegal goods, services, or content online. In particular, platforms must implement policies to ensure greater traceability of business users in online market places and must provide a mechanism for any individual or entity to easily flag illegal content. Requirements for various categories of intermediaries include:

- Providers of intermediary services must *respond to government orders* to take down illegal content or to provide information about a specific user. The response must include information about the redress available to the provider of the service and to the user (Arts. 8, 9).
- Providers of intermediary services must publish an *annual transparency report* on how content is removed, why it was removed, how much is removed, the accuracy of automated content moderation, and any safeguards applied (Art. 13).
- Users of hosting services must be able to easily *flag illegal content*, such as offers to sell illegal goods, illegal hate speech, terrorist content, and unlawful discriminatory content (Arts. 14, 19).
- Providers of hosting services must *notify authorities* where they become aware of a "criminal offence involving a threat to life or safety" (Art. 15a).
- Providers of online platforms must provide an *appeal process* for users to challenge platforms' content moderation decisions and seek redress, including through an out-of-court dispute mechanism (Arts. 17(4), 18).

- Providers of online platforms must comply with additional *Know Your Customer* ("KYC") guidelines on sellers that use the platform to offer products or services (Art. 24c-e).

- Providers of online platforms "accessible to minors" must put in place "appropriate and proportionate measures to *ensure a high level of privacy, safety, and security of minors*, on their service" (Art. 24b).

Transparency Requirements

The DSA also establishes stringent transparency requirements for intermediary services regarding targeted advertising and content moderation practices. Requirements for various categories of intermediaries include:

- Providers of intermediary services must provide *terms and conditions* in "user-friendly" language outlining their content moderation, algorithmic decision-making, human review, and internal complaint handling system procedures (Art. 12);

- Providers of intermediary services must publish *annual reports* on any content moderation, including the number of complaints received, the number of disputes submitted to out-of-court dispute settlement bodies, and the median time needed for completing such settlement procedures, and the number of suspensions enacted by the platform (Art. 13);

- Providers of hosting services must *inform users* when removing or disabling their content or access and provide specific reasons to affected users (Art. 15);

- Providers of online platforms that engage in *targeted advertising* must provide to users information on the criteria used to determine what advertisements are presented to specific users and on whose behalf each advertisement is being presented (Art. 24), and enable users to refuse or withdraw from such advertising, without being denied access to the service (Recital 52); and

- Providers of online platforms that use *recommender systems*—defined as a fully or partially automated system that is used to suggest, prioritize or curate specific information to users—set out in the terms and conditions the main parameters used in those algorithms, including the criteria, relative importance of those criteria, and information on how the user's behavior impacts recommendations (Art. 24a).

Requirements for VLOPs

The DSA provides that VLOPs (such as major social media platforms) have "a systemic impact in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas." Accordingly, the DSA imposes additional, more stringent obligations on them. In addition to the requirements listed above, VLOPs will be subject to the following obligations:

Greater Transparency Requirements

- For *targeted advertising*, platforms must display the identity of the advertiser and provide information about the "main parameters" used in targeting (Art. 30); and keep a publicly available repository of online advertisements displayed by the platform, including details of which user groups were targeted by each advertisement (Art. 30).

- For *recommender systems*, platforms must allow users at least one choice of algorithm that is not based on behavioral profiling (e.g., a chronological feed), as well as enabling them to easily select or modify that alternate option at any time (Art. 29).

- Platforms must publish a comprehensive *transparency report* every six months that includes information on how content is removed, why it was removed, how much is removed, the accuracy of automated content moderation, and any safeguards applied (Art. 33).

Risk Management and Risk Assessments

- Platforms must implement a *risk management system* that identifies, analyzes and mitigates "systemic risks" on the platform (see below), and which will be subject to external independent auditing (Arts. 26, 28).

- On the date the DSA enters into force for VLOPs, at least once a year thereafter, and before launching new "functionalities," platforms must *identify and assess any significant systemic risks*, including:

    - dissemination of illegal content;

    - negative effects for fundamental rights, including for consumer protection, private and family life, protection of personal data, freedom of expression and information, the prohibition of discrimination, and the rights of the child;

- negative effects on public health, minors, civic discourse, electoral processes and public security;
- the extent to which these risks are influenced by the intentional manipulation of their service; and
- the extent to which the use of algorithmic systems impacts these risks (Art. 26).

- Platforms are required to take reasonable, proportionate and effective *mitigation measures*, tailored to identifying systemic risks identified by the risk management system (Art. 27).
- Platforms must provide *annual public reporting* on results of risk assessment and mitigation measures (Arts. 26, 27 and 33).
- Platforms must comply with *voluntary "codes of conduct"* (to be drafted at a later date) for addressing systemic risks (such as the spread of disinformation or negative effects on democracy and human rights) and undergo annual audits for compliance (Art. 35).

Platforms must comply with ***crisis response protocols*** developed by the Commission in the event of a "serious threat to public security or public health," which may include ordering the platform to "identify and apply specific, effective and proportionate measures" of the platform's choice to mitigate the threat, provide information on the threat, or report back to the Commission on progress in mitigating the threat progress (Art. 27a).

Platforms must conduct ***external independent auditing*** of the platform's compliance with the DSA on an annual basis, by auditors with proven expertise, technical competence, and capabilities in the area of risk management (Art. 28).

Platforms must ***provide access to platform data*** to regulators and vetted researchers under certain circumstances (Art. 31).

Enforcement

For **most platforms**, national-level authorities will be primarily responsible for enforcement of the DSA, with support from the newly formed European Board for Digital Services. Member states will each authorize an authority as a Digital Services Coordinator, which shall be responsible for all matters relating to supervision and enforcement of the DSA. Digital Services Coordinators will have the power to, among

other remedies, impose fines of up to 6% of the annual worldwide turnovers of providers who fail to comply with DSA obligations.

For **VLOPs**, however, the European Commission will be primarily responsible for the supervision and enforcement of the DSA, and will be granted enhanced powers for this purpose. The Commission may impose fines of up to 6% of the platform's annual global turnover where it finds an infringement or failure to comply. Other specific powers include the authority to request information from the platform (Art. 52); conduct on-site inspections (Art. 54); and initiate monitoring actions, wherein the Commission can order a platform to provide access to, and explanations relating to, its databases and algorithms (Art. 57).

Conclusion

The DSA is a groundbreaking legislation that aims to transform the digital regulatory landscape in the EU and beyond. In order to be prepared to comply with the new rules, companies will need to take note of additional compliance or reporting requirements that the DSA will create for them, and the tight timeline on which they will need to remedy any compliance gaps. Companies should pay special attention to any implications for their advertising platforms as well as any use of algorithmic decision-making or AI, especially in the context of content moderation and recommender systems, as those applications will be subject to unprecedented transparency requirements and, as a consequence, regulatory scrutiny.

The authors would like to thank Law Clerk Melissa Muse and Summer Law Clerks Josh Goland, Sharon Shaji, and Annabella Waszkiewicz for their contributions to this article.

To subscribe to our Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Michael Pizzi
mpizzi@debevoise.com