Updates
October 10, 2022
The EU’s Digital Services Act: A Paradigm Shift for Online Intermediaries

Following the European Council's approval last week, the Digital Services Act (DSA) has been officially adopted, starting the countdown to the law's entry into force later this year. The DSA builds on the Electronic Commerce Directive 2000 (e-Commerce Directive) and regulates the obligations of digital services that act as intermediaries in connecting consumers with third-party goods, services, or content.

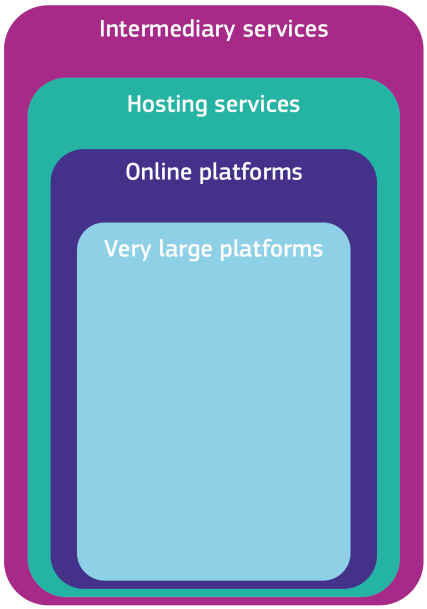
The DSA is a paradigm-shifting law that features due diligence and transparency obligations for all online intermediaries. In addition to the more commonly seen notice-and-takedown and transparency requirements for "illegal content," the DSA contains novel and extensive obligations related to global content moderation, advertising, data access, and product design practices.

The European Union (EU) has adopted the DSA in reaction to perceived societal and consumer risks posed by online platforms and other digital intermediaries. The goals of the law are to (1) protect consumers' fundamental rights through a safe, predictable, responsible, and trustworthy online environment; (2) establish a single EU-wide framework governing providers and platforms; and (3) foster innovation and competitiveness.

Providers in Scope

All intermediary service providers that store, transmit, or disseminate user-generated content and have a substantial connection to the EU are subject to the DSA. Providers' specific obligations, however, depend on their size and type of service. The DSA's classification scheme is below.

- All intermediary services, including the following:
  - "Mere conduit" intermediary services that transmit information in, or provide access to, a communication network (e.g., internet exchange points).
  - "Caching" intermediary services that transmit information together with automatic/temporary storage for the purpose of making the information's transmission more efficient (e.g., reverse proxies).



- Hosting services that store information provided by recipients of the service (e.g., web or cloud services).
- Online platforms: hosting services that store recipient information and disseminate information provided by recipients to the public by request (e.g., social networks, online marketplaces).
- Very large online platforms (VLOPs) and search engines: online platforms that provide their services to more than 45 million recipients in the EU, as determined by the European Commission, the executive body of the EU.

The graphic on the right, created by the European Commission, illustrates the DSA's "nested" structure.

Noteworthy Requirements by Category of Provider

All intermediary services are subject to a minimum level of obligations. The DSA then imposes additional and cumulative obligations on hosting services, online platforms, and very large online platforms.

Requirements for All Intermediary Service Providers

- **Terms and conditions transparency.** All intermediaries must specify any restrictions imposed on the use of their service, including information on the policies, procedures, tools, and algorithms used for content moderation and internal complaint handling. Any content restrictions must be enforced in an objective and proportionate manner, with due regard for fundamental rights.
- **Annual reporting.** All intermediaries must produce annual reports that include (1) information on the number of orders issued to provide information and/or take down illegal content, and (2) information on content moderation undertaken, including on the use of account suspension, content removal, automation, downranking, and visibility filtering, categorized by the type of illegal content or terms and conditions violation.
- **Compliance with government orders.** All intermediaries must comply with orders from EU member state authorities to provide information or to act against illegal content.
- **Single point of contact.** All intermediaries must designate a single point of contact for member state authorities.

Requirements for Hosting Services (Including Online Platforms)

- **Statement of reasons for all content moderation (except certain categories of spam).** Hosting providers must provide a clear and specific statement of reasons for any visibility filtering, downranking, content removal, demonetization, or account suspension. The statement must include, among other things, the basis for the decision and, where applicable, information on the use of automation.
- **Notice-and-action mechanisms.** Hosting providers must enable (a) submission by anyone via an easy-to-access, user-friendly, electronic mechanism notices containing a substantiated explanation as to why specific content is allegedly illegal under EU or member state law (along with additional transparency reporting on these mechanisms); and (b) adjudication of notices in a timely, diligent, nonarbitrary, and objective manner, along with notification to the submitting party of the decision made.
- **Reporting criminal offenses.** Upon becoming aware of any information giving rise to a suspicion that a serious criminal offense involving a threat to life or safety of persons has taken place, providers must promptly inform law enforcement or judicial authorities in the relevant EU member state and provide all information available.

Requirements for Online Platforms

- **Recommender system transparency.** Platforms must describe, in their terms and conditions, any parameters used to suggest information to users, and they must disclose options to modify those parameters.
- **Protection of minors.** Platforms must put in place appropriate and proportionate measures to protect the privacy, safety, and security of minors. Platforms are also prohibited from serving ads based on the profiling of minors.
- **Mandatory suspension.** Platforms must suspend, for a reasonable period of time, after having issued a warning, users that frequently provide "manifestly illegal" content, as well as the processing of notices by individuals or entities that frequently submit manifestly unfounded complaints.
- **Advertising transparency.** Platforms must ensure that users are able to obtain specified information for each advertisement displayed.
- **Online interface design.** Platforms may not design, organize, or operate their service in a way that deceives, manipulates, materially distorts, or impairs users' ability to make free and informed decisions.
- **Special obligations for marketplaces.** Before allowing an online marketplace, platforms must obtain identifying information from traders and make it available to users. Platforms must also periodically check for the availability of illegal products or services and notify users when such products or services are detected.
- **Internal complaint-handling system and out-of-court dispute settlement.** Platforms must maintain an appeals system allowing decisions taken against allegedly illegal content, terms and conditions violations (such as content removal, account suspension, and/or service termination) to be challenged for up to six months and reversed. For issues that are not satisfactorily resolved by their internal system, platforms must participate in out-of-court dispute settlement proceedings. The availability of out-of-court dispute settlement is without prejudice to users' ability to challenge content decisions in national courts.
- **Trusted flaggers.** Platforms must create a channel through which trusted flaggers can report illegal content for priority review and action.
- **Additional transparency obligations.** The DSA outlines additional transparency obligations for online platforms on the above requirements, including submission of moderation decisions and statements of reason (excluding personal data) to the European Commission for inclusion in a publicly accessible database.

Requirements for VLOPs

- **Risk governance obligations include the following:**
    - **Annual systemic risk assessments.** VLOPs must undertake annual assessments of the severity and probability of the following: (1) dissemination of illegal content; (2) negative effects on fundamental rights, including human dignity, privacy, freedom of expression and information, freedom and pluralism of the media, nondiscrimination, rights of the child, and consumer protection; (3) negative effects on civic discourse, electoral processes, or public security; and (4) gender-based violence, negative effects on public health and on minors, and serious negative consequences to a person's physical and mental well-being.
    - **Risk mitigation measures.** VLOPs must put in place reasonable, proportionate, and effective risk mitigation measures tailored to the specific systemic risks identified.
- **Crisis response.** Where the European Commission determines that a threat to public security or public health exists, VLOPs may be required to assess how their platforms contribute to the threat and implement mitigation measures.
- **Independent audits and compliance function.** VLOPs must undergo annual independent audits to assess compliance with certain DSA obligations and establish an internal compliance function dedicated to monitoring DSA compliance.
- **Data access.** VLOPs must provide member state authorities and vetted researchers with access to certain types of data, including on the design, functioning, and testing of algorithmic systems.
- **Additional transparency obligations.** Transparency reporting obligations for VLOPs include publishing reports on content moderation every six months and creating an anonymized repository for advertising information.

Penalties and Enforcement

The DSA imposes steep penalties for noncompliance. The maximum penalty for a failure to comply with the DSA's substantive obligations is 6% of a provider's global annual gross revenues. A "periodic penalty" for noncompliance may also be imposed, not to exceed 5% of a provider's average daily turnover in the preceding financial year. Where a provider supplies incorrect, incomplete, or misleading information to a regulator, the provider may be subject to a maximum fine of 1% of global annual gross revenues.

The DSA empowers national-level regulators, including digital services coordinators (DSCs), to supervise, investigate, and enforce the DSA. DSCs will have the authority to, among other things, issue investigative orders, impose fines, and order intermediaries to remedy infringements. In cases of persistent or systematic noncompliance, DSCs will have the authority to order the temporary restriction of access to the infringing service or provider. For VLOPs, DSCs will be empowered to refer systematic noncompliance to the European Commission for further investigation. The commission may initiate proceedings against and investigate VLOPs, issue and monitor interim measures, and, as necessary, impose fines.

Entry Into Force and Next Steps

The DSA will enter into force 20 days after its publication in the *Official Journal of the European Union* later this fall. Once the DSA is in force, all online platforms (except for small/micro platforms) will be required to publish their number of average monthly active recipients. Several DSA articles and recitals should inform this calculation. The recipient numbers will enable the commission to determine which providers meet the threshold of 45 million recipients needed to qualify as a VLOP.

The entry-into-force date will also start the clock on the law's date of application to all intermediaries (likely between January and March 2024) and its earlier date of application to those platforms designated by the European Commission as VLOPs (likely between February and July 2023). From their respective dates of application, intermediaries will be subject to investigations and enforcement by the commission and EU member states' DSCs.

Compliance strategies for the DSA will vary depending on the provider's services, products, and processes. While all intermediaries will need to assess gaps in compliance and consider policy and product updates, in certain circumstances, relatively straightforward updates may suffice to satisfy the provider's obligations and mitigate risk. In other cases, designing and implementing process-driven governance systems may be advisable to provide enduring risk mitigation. Companies offering online services in the EU should speak with experienced counsel to understand the obligations they may have under the DSA.

As part of Perkins Coie's Privacy & Security practice, our lawyers work with the world's most innovative companies on a range of regulatory, product, risk governance, and human rights matters.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security Communications

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law