

## BEYOND VLOPS AND GATEKEEPERS:

### Countdown to the full application of the EU Digital Services Act (DSA)

19 September 2023

---

The Digital Services Act (DSA) is set to overhaul and expand the EU's regulatory framework for online intermediary services. While very large online platforms and search engines (VLOPS / VLOSES), such as Amazon Store, Facebook or Google Search, have been subject to the new rules since August 2023, the DSA will become fully applicable for all covered services on **17 February 2024**. Given the DSA's broad scope of application, this will trigger various new compliance obligations for a wide range of digital businesses. With only five months left, the clock is ticking to implement the comprehensive requirements.

#### 1 What is the DSA?

Together with the Digital Markets Act (DMA), the DSA constitutes a cornerstone of the EU's ambitious Digital Services Package, a set of directly applicable rules aiming to modernise and further harmonise the regulatory framework for digital services across the EU. While the DMA regulates the largest online platforms (so-called "gatekeepers") from a competition law perspective, the DSA introduces specific transparency and accountability requirements for digital services that act as intermediaries in their role of connecting users (both consumers and businesses) with goods, services and content.

The DSA aims to achieve its objectives by essentially following a three-tiered approach that includes:

- (i) a revised liability "safe harbour" regime for intermediary services (Chapter II),
- (ii) increased due diligence and transparency obligations for providers (Chapter III), and
- (iii) enhanced enforcement powers and cooperation mechanisms for the EU Commission and Member State authorities (Chapter IV).

DSA compliance is underpinned by a dual system of sensitive administrative sanctions and private enforcement. Namely, DSA infringements are subject to maximum fines of up to 6% of the service provider's annual worldwide turnover. Furthermore, individual users may seek compensation for (both material and non-material) damages suffered as a result of DSA infringements.

#### 2 Which services will be covered by the new rules?

The DSA is regularly discussed solely in the context of Big Tech and so-called gatekeepers, while many overlook the regulation's broad scope of application. In fact, any digital business dealing with third-party content could potentially be affected (e.g., cloud services, web-shops, blogs or communication services), irrespective of their size

Wolf Theiss

and reach. As such, already seemingly benign activities, like the inclusion of a comment section or chat function on a website, may suffice to trigger the DSA's application.

Specifically, the DSA defines the following regulated intermediary services:

- **"Hosting"** services offer storage infrastructure for user-provided information. This category covers a wide range of services, including cloud computing, web hosting, referencing services, as well as file storage and sharing. **"Online platforms"** that not only store but also publicly disseminate user-provided information constitute a special sub-category with heightened compliance requirements (e.g., online marketplaces, comparison portals, social media).
- **"Mere conduit"** services merely transmit user-provided information in a communication network or provide access thereto. Examples include internet exchange points, wireless access points, VPNs, DNS services, top-level domain name registries, as well as voice over IP and other interpersonal communication services.
- **"Caching"** services transmit user-provided information, while also including the automatic, intermediate and temporary storage of the information for efficiency purposes. Examples include content delivery networks, reverse proxies or content adaptation proxies.
- **"Online search engines"** allow users to submit queries to perform online searches in the form of keywords, voice requests or other input.

The DSA's territorial scope follows the market-place principle. Hence, the regulation applies to intermediary services offered to users within the EU, irrespective of where the provider is established. Many non-EU service providers will thus have to ensure DSA compliance by 17 February 2024 as well.

### 3 What are the key compliance obligations under the DSA?

The DSA follows a graduated approach, introducing different requirements depending on the type and size of the respective service provider. For instance, online platforms are subject to different (heightened) compliance obligations compared to "regular" hosting services. Key DSA requirements include the following:

- **Handling unlawful content:** The DSA requires service providers to implement effective systems to combat unlawful user-provided content, which entails *inter alia* increased cooperation with public authorities (Art 9 and 10). Moreover, hosting providers are required to report potential criminal offenses (Art 18) and to establish effective notice-and-action and redress mechanisms (Art 16). These requirements are accompanied by revised liability exemptions for intermediary service providers (Art 4 – 8 DSA), which are modelled after the existing safe harbour regime under the E-Commerce Directive and codify respective CJEU case law. In essence, hosting providers thus remain liable for unlawful third-party content only if they have actual knowledge or awareness of unlawful content and do not act expeditiously to block or remove it.
- **Points of contact and legal representatives:** Intermediary service providers must also designate a single point of contact vis-à-vis authorities and users (Art 11 and 12). Non-EU providers must designate a sufficiently authorised and resourced legal representative within the EU (Art 13).
- **Updated terms and conditions:** Intermediary service providers will need to revise their terms and conditions to include information on restrictions in respect of user-provided information (Art 14). This may include information on content moderation policies, measures and tools, including algorithmic decision-making and human review.
- **Transparency reports:** At least once a year, intermediary service providers shall make detailed reports on their content moderation practices (Art 15) publicly available. Depending on the type of provider, different specifications apply.

- **Internal complaint-handling system:** Online platforms must establish an internal complaint-handling system, which allows users to complain *inter alia* about content removal, account suspension and other content moderation decisions undertaken by the provider (Art 20).
- **"Dark patterns," targeted advertising and recommender systems:** The DSA introduces specific restrictions concerning user targeting and other forms of (marketing) communication. This includes the prohibition of so-called "dark patterns" (e.g., nudging or misdirection) (Art 25 and 31), increased advertising transparency, including the disclosure of targeting parameters (Art 26), as well as bans on certain types of profiling-based advertisement (Art 26 and 28). By the same token, online platforms using recommender systems (e.g., in their content feed) are required to publish the system's main parameters and information on options to modify or influence said parameters (Art 27).
- **Protection of minors:** Online platforms accessible to minors must also implement adequate measures to ensure a high level of privacy, safety and security of minors (Art 28).
- **Know your business customer (KYBC):** Providers of B2C online marketplaces are *inter alia* required to collect contact, identification and payment data from traders based on the know-your-business-customer principle (Art 30).

Needless to say, the above constitutes merely a selective sub-set of the DSA's comprehensive new requirements. In addition, partial exemptions may apply for small and micro enterprises (fewer than 50 employees and less than EUR 10 million in annual turnover).

#### 4 Time to Act!

In light of the comprehensive new requirements, and with only five months left until the 17 February 2024 deadline, digital businesses should now start to assess whether and to what extent the DSA will apply to them. Should existing compliance gaps be identified, the necessary measures will then need to be implemented by the aforementioned deadline. Since this will in many cases require significant organisational, technical and legal efforts, including the involvement of different business stakeholders, sufficient preparation time should be afforded to this project.

Our experts in all 13 Wolf Theiss jurisdictions are happy to assist you with every step along the way.

## About Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With more than 360 lawyers in 13 countries, over 80% of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

**For more information, please contact:**



**Georg Kresbach**  
Equity Partner

**E** [georg.kresbach@wolftheiss.com](mailto:georg.kresbach@wolftheiss.com)

**T** +43 1 51510 1090



**Phillip Wrabetz**  
Senior Associate

**E** [phillip.wrabetz@wolftheiss.com](mailto:phillip.wrabetz@wolftheiss.com)

**T** +43 1 51510 1097



### Sign up

to receive our  
latest updates  
and insights