The Digital Services Act: Answers to 10 questions that SaaS companies should be asking themselves now

October 24, 2024

*Regulation (EU) 2022/2065, the so-called Digital Services Act ('**DSA**', available here), came into force on November 16, 2022 as part of the larger EU Digital Strategy (including the Digital Markets Act, Data Act and AI Act) and became fully applicable on February 17, 2024. It is intended to create a harmonized EU legal framework ensuring a safe, predictable and trusted online environment. To this end, it provides for numerous obligations, but also liability reliefs for intermediary services. SaaS companies with often heterogeneous and difficult-to-classify business models, in particular, need to consider what their obligations are and how they must act now. In this context, certain misconceptions prevail which, in the worst case, may give rise to liability risks. The following article seeks to address key questions and clarify the most common misunderstandings.*

1. What are the aims of the DSA?

The DSA has various aims: It is intended to promote electronic commerce and create a harmonized internal market free of national barriers by establishing uniform rules. This should ease the development of innovative digital services for companies and offer consumers a wide range of competing services.

Furthermore, platforms are to be regulated more effectively and consistently in order to counteract the specific and systemic risks inherent in the digital economy more adequately. In particular, the **spread of illegal content is to be contained** and in addition, **clearer guidelines for platforms are to be established**.

2. To whom does the DSA apply?

There is a widespread misconception that the DSA only applies to very large platforms. It is true that the DSA has a tiered approach to obligations, with special, more extensive obligations for very large online platforms (so-called '**VLOPs**') and very large online search engines (so-called '**VLOSEs**') with more than 45 million users per month in the EU. However, according to Art. 2 para. 1, the DSA applies to any type of intermediary service regardless of its size. The term 'intermediary service' (defined in Art. 3 lit. (g)) covers three categories of services: mere conduit, caching and hosting services.

The category 'hosting services' is ff particular importance for SaaS companies - the term is defined very broadly. It includes any service whose purpose includes '**storing information provided by users on their behalf**'.

In doing so, the DSA does not take a service provider-specific view, but rather a **service-related view**. For companies, this means that different services may fall under different areas of the DSA. In this case, a precise demarcation and analysis is indispensable. It should also be noted that the so-called **market place principle** also covers companies without an establishment in the EU, as long as they **offer services in the EU** (Art. 2 para. 1, 3 lit. (d) and (e) DSA).

3. What subcategories of hosting services exist under the DSA and how do they relate to each other?

While hosting service providers are 'only' subject to the general obligations in Art. 11-18, the DSA's tiered concept of obligations recognizes **subcategories** of hosting service providers that are subject to a more extensive catalogue of obligations:

- **Online platforms** (Art. 3 lit. (i) DSA), such as hosting services that not only store information on behalf of a user but also **publicly disseminate** it, i.e. make it available to a potentially unlimited number of third parties, are subject to the further obligations set out in Art. 20-28 DSA.
- Providers of online platforms allowing consumers to conclude distance contracts with traders (hereinafter: '**online trading platforms**') are subject to the general and online platform obligations in addition to the obligations in Art. 30-32 DSA.

4. What examples of services are conceivable?

Based on the abstract description given above, the group of **hosting services** typically encompasses various types of **cloud computing services**, regardless of whether the service is limited to offering storage space (as with Dropbox or Google Drive) or computing power or whether it includes certain software or other additional features.

The narrower category '**online platforms'** contains **social media services** (such as Facebook, LinkedIn or Instagram) and, in some cases, **instant messaging services** (e.g. Telegram). In addition to these typical cases, however, any SaaS companies that offer users the opportunity to make content they have posted accessible to a large number of other users are likely to be covered. Marketplaces, i.e. platforms where users offer goods or services (such as eBay or Amazon Marketplace), fall under the even narrower category of **online trading platforms**.

At the same time, if an activity is, for example, a minor and purely ancillary feature of another service, or a minor functionality of the principal service, it is not considered an online platform under the DSA. This requires service providers to check on a case-by-case basis whether an exception may apply.

5. What does this mean for start-ups and SMEs?

For small and micro-enterprises, the implementation of the DSA can sometimes lead to a disproportionate burden, for example, due to its requirements regarding organizational and procedural obligations. This has also been recognized by the legislator. The special due diligence requirements for online platforms and online trading platforms therefore **do not apply, or only to a limited extent,** to small and micro-enterprises (see Art. 19, 29 DSA). Whether or not a company reaches the thresholds set for this must be examined on a case-by-case basis.

6. Does the DSA only apply to B2C services?

The term 'recipient of the service' and the fact that the DSA (at least also) serves to protect consumers initially **suggest that** the DSA only applies when information is provided to consumers.

However, the DSA has a very broad understanding of the term and, with Art. 3 lit. (b), covers any **natural or legal person** who uses an intermediary service, in particular for the purposes of seeking information or making it accessible. Therefore, in addition to **B2C** platforms, pure **B2B** platforms are also covered by the DSA.

7. When are hosting service providers liable for illegal content posted by their users?

Compared to the previous legal situation, the regulations on liability privileges for intermediaries remain largely the same. Providers of hosting services are still **generally not responsible** for information provided by a recipient of the service as long as they **do not** have actual knowledge about the illegality or, with regard to claims for damages, the facts/circumstances from which an illegality is apparent. Additionally, there is still **no general obligation to monitor content**, Art. 8 DSA.

As soon as a provider becomes aware of illegal content, they must **act expeditiously** to **remove** the content or to **disable access** to it, Art. 6 para. 1 lit. (b) DSA (so-called notice-and-takedown procedure). In this context, **knowledge** is already (refutably) **presumed** if the provider has received a **substantiated notice** – for example, from another user – cf. Art. 16 para. 3 DSA. For this purpose, hosting service providers are obliged under Art. 16 DSA to provide **appropriate notice and action mechanisms** within their service. Any further voluntary, unfounded investigation of user content is possible and does not affect the liability exemption (so-called '**good samaritan privilege**', Art. 7 DSA).

However, providers are no longer privileged if they take an **active role** with regard to user content. If a provider gains knowledge of or control over the content, e.g. by **editorially** reviewing or selecting the content before storing or transmitting it, they are also liable if the content is illegal. To determine when a specific provider takes an active role, a detailed case-by-case analysis will generally be required. However, an active role is not taken simply by voluntarily checking for possible illegality of user content without any specific reason (so-called '**good samaritan privilege**', Art. 7 DSA). It is only when illegal content is discovered that a provider needs to act quickly – thus, gaining knowledge through voluntary checks is not treated differently than knowledge gained from receiving information from users.

8. What other due diligence obligations must be complied with regarding illegal content?

All hosting service providers must, as part of their **general obligations** (Art. 11-18 DSA), set up a central point of contact for authorities (Art. 11 DSA) and recipients of the service (Art. 12 DSA) in order to enable rapid, electronic and user-friendly communication. Providers without an establishment in the EU shall designate a legal representative in the EU (Art. 13 DSA). Furthermore, an annual report on the management of reports and complaints must be published (Art. 15 DSA) and, in the event of suspicion of a **criminal offence** involving a threat to the security of a person, content must be reported to law enforcement authorities (Art. 18 DSA). **Online platforms** also have stricter obligations to receive and respond to reports, in particular from so-called trusted flaggers, and to take action in the event of abuse (Art. 22 and 23 DSA). **Online trading platforms** must also ensure to a greater extent that providers can be identified and do not offer illegal products or services by designing the platform appropriately, implementing technical measures and conducting regular spot checks. In addition, affected consumers must be informed if they have been affected by illegal content (Art. 30-32 DSA).

If content is deleted or blocked, hosting service providers must **provide** the recipients of the service concerned with a clear and specific **statement of reasons** for such actions (Art. 17 para. 1, 3 and 4 DSA). **Online platforms** must also provide recipients of the service effective options for legal defense, i.e. in particular, they must allow complaints to be made against measures that have or have not been taken and they must decide on these complaints in a timely, non-discriminatory, diligent and non-arbitrary manner (Art. 20 and 21 DSA).

9. What must be taken into account when designing the SaaS solution and drafting and enforcing user agreements?

All **hosting service providers** are obliged to draft their contracts in a **transparent and comprehensible manner** and to **enforce them in a diligent, objective and proportionate**

manner. Recipients of the service must be able to understand, among other things, when content is deleted, or accounts are blocked (Art. 14 DSA) and how user complaints are handled (Art. 23 DSA).

Online platforms that use (algorithmic) **recommender systems**, i.e. that sort user content and display it to specific recipients of the service, must disclose how they work and make it possible and recognizable to choose the preferred recommender system (Art. 27 DSA). Platforms shall not be designed in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions (so-called `**dark patterns**´, Art. 25 DSA). Advertisements displayed must be clearly labelled and the reason for their display must be disclosed to the individual recipient of the service (Art. 26 DSA). If the recipient of the service is a recognizable minor, further restrictions apply (Art. 28 DSA).

10. What are the sanctions for violating the DSA?

The DSA follows the principle of **two-pronged enforcement**, which has been utilized by various EU legislative acts in recent years.

On the one hand, violations can be penalized by the competent **national authorities** or the so-called `**Digital Services Coordinator**´ (Art. 49 para. 2 DSA; in Germany, the Federal Network Agency, *Bundesnetzagentur*). The full range of instruments for requesting information, taking corrective action and imposing sanctions as set out in Art. 51 DSA is available to them. Depending on the specific infringement, fines can amount to up to 1% or 6% of the annual worldwide turnover (Art. 52 para. 3 DSA). As a particularly restrictive measure a **temporary restriction of access** to the service concerned may be imposed (Art. 51 para. 3 lit. (b) DSA).

On the other hand, violations can also be enforced through private legal action. According to Art. 53 DSA, affected recipients of the services have the right to lodge a complaint with the Digital Services Coordinator against providers of intermediary services and, if necessary, to obtain an administrative order. In addition, they are free **to seek compensation** in the form of damages, in accordance with the national law, pursuant to Art. 54 DSA. Furthermore, DSA violations may, under certain circumstances, constitute unfair practices under Sec. 3a of the German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*), which allows competitors and consumer associations, among others, to issue cease and desist letters. In view of this, SaaS companies should not rely on idle supervisory authorities.

This article shows that SaaS companies are in most cases subject to the DSA. However, the exact categorization and examination of services as well as possible exceptions can be complex. At the same time, the specific classification can have significant time-consuming and costly effects, since it determines whether only the general obligations for hosting services apply or whether, for instance, an internal complaint management system and technical design measures must be established and implemented. The design of a service along with the targeted definition and consistent enforcement of contractual terms of use, can therefore play an important yet often underestimated role in avoiding more far-reaching obligations and minimizing liability risks. We are happy to advise on this and general compliance issues.