

## Digital Services Act (DSA) Explainer

### *What is the DSA?*

The Digital Services Act (DSA) is a new law in the European Union (EU) that aims to create a safer online environment by defining clear responsibilities for all online intermediaries and platforms. In short, the DSA will hold search engines, social media networks, and marketplaces accountable for policing content on their sites.

The DSA revises the 20-year-old eCommerce Directive which acted as the foundational legal framework for online services in the EU until now. While the eCommerce Directive exempted intermediaries from liability for the content they host if they meet certain conditions, the online environment today is drastically different from 20 years ago. New digital businesses that play an increasingly important role in our daily lives have emerged. Therefore, the European Commission concluded that redefining responsibilities for all online actors was necessary.

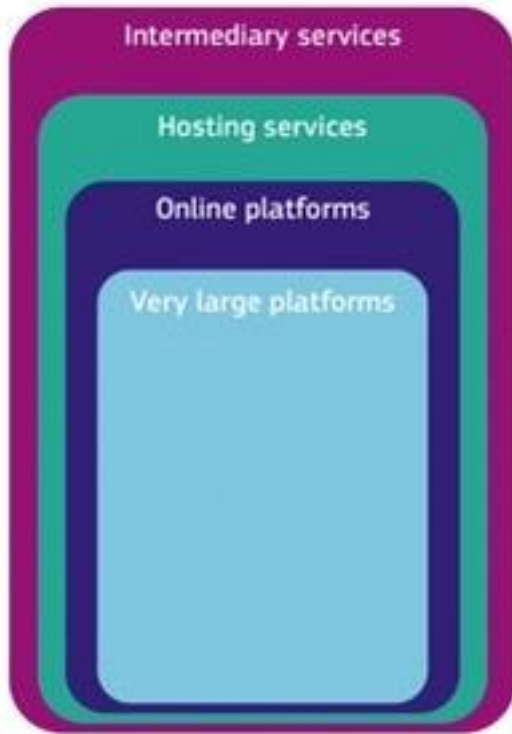
The DSA seeks to tackle current challenges of the digital ecosystem such as illegal products, hate speech, or disinformation, as well as transparent data reporting and oversight. To achieve these goals, the DSA will impose rules to regulate how platforms moderate content, advertise online, and use algorithmic processes. For example, online platforms must clearly explain how their recommendation system works, like why a user is being shown cat photos or other types of (potentially more controversial) content. The largest online platforms will also need to assess the risks their systems pose to the public interest or fundamental rights, such as disinformation, cyber violence against women, or harms to minors online and take action to prevent abuses.

Additionally, the DSA maintains the fundamental principles applicable to e-commerce in the EU, including exempting platforms from being liable for any illegal content they host, as long as they take action against illegal content, they are aware of and don't deliberately contribute to the dissemination of illegal content.

### *Does the DSA apply to small businesses?*

The short answer is yes. The DSA applies to all online intermediaries offering services to users in the EU, irrespective of the service provider's place of establishment. **However, small and medium-sized enterprises (SMEs) will be exempt from the costliest obligations (see below).**

The law proposes a *gradual regime*, depending on the role, size, and impact of different online players in the online ecosystem. As such, the DSA distinguishes between online intermediaries, hosting services, online platforms, very large online platforms, and marketplaces:



**Intermediary services** encompass most information society services. They consist of the mere transmission of user information in a communication network, including the automatic, intermediate, and temporary storage of that information.

**Hosting services** are services that store information provided by and at the request of a user of the service.

**Online platforms** are hosting services which, at the user's request, store and disseminate information to the public. A special category in the DSA includes **marketplaces**, which are online platforms that allow consumers to conclude distance contracts with traders.

**Very large online platforms (VLOPs) and search engines (VLSEs)** are online platforms which reach 45 million or more monthly users in the EU. The European Commission must designate VLOPs and VLSEs as such before they become subject to the Commission's direct supervision and more stringent requirements.

Picture credits: European Commission

**Will small developers have to comply with the DSA obligations?**

While the DSA will make it easier for small app developers and tech SMEs to comply with a single set of EU rules applicable to all, they will have to carefully consider certain new provisions when developing and placing apps on the market.

The DSA foresees more stringent rules for VLOPs/VLSEs and exempts micro and small enterprises from certain obligations, including transparency reporting requirements. The exemption also applies to micro and small enterprises that lost their small business status during the past 12 months.

However, the DSA also creates some disadvantages for SMEs that are not established in the EU. They will, for example, need to appoint a legal representative in the EU, which entails additional costs.

Below we summarise some of the most important obligations for small and micro enterprises. We listed all the obligations the DSA imposes on online platforms at the end of this document.

*The most relevant provisions for app developers*

DSA Obligations	What does this mean for app developers?
Providers of online intermediaries outside the EU need to appoint a legal representative in one of the Member States where they offer services (Article 11)	The DSA rules apply in the EU single market, without discrimination, including to those online intermediaries established outside of the EU that offer their services in the single market. This means that app developers established outside of the EU, for example, in the United States or elsewhere, will have to appoint a legal representative in the EU. Doing this will allow them to benefit from the liability exemptions and enable them to adhere to a single set of rules when providing their services in the EU.

	<p>This obligation is similar to the concept of the EU representative in the General Data Protection Regulation (GDPR). However, the DSA representative can be held liable for non-compliance with the regulation and, therefore, is not a role to be taken lightly.</p> <p>The cost of such representation can be a burden for smaller companies. Fortunately, it is possible that a legal representative is appointed, in accordance with national law, by more than one provider of intermediary services. This would allow SMEs to pool their resources to collectively designate a representative.</p>
<p><b>Hosting services and online platforms must implement 'notice and action' mechanisms (Article 14)</b></p>	<p>Providers of hosting services must implement mechanisms to allow any user or entity to notify them of the presence of content that is considered illegal on their service. The hosting service needs to confirm receipt of submitted notices without undue delay and notify the user of its decision with respect to the information to which the notice relates. Hosting services can use automated means for the processing of the notices and the decision-making related to the action.</p> <p>App developers will have to put in place and maintain mechanisms allowing users to flag illegal content. The maintenance of the system and the review of submitted notices can drain both human and financial resources. Serious review of user-submitted notices will be crucial, as these notices can give rise to actual knowledge or awareness of illegal content on the platform. App developers could, therefore, be liable for the illegal content on the platform if they don't take action.</p>
<p><b>Hosting services have to provide a statement of reasons to users for any actions restricting their use of the service (Article 15)</b></p>	<p>Hosting providers will need to provide a statement of reasons to users on any imposed restrictions concerning the visibility or removal of content, the suspension, termination or other restrictions of monetary payments, as well as the suspension or termination of the service or a user's accounts.</p> <p>Hosting services will have to dedicate resources to notifying and explaining to users why and how they are affected by restrictions imposed on them. The information provided to users should mention clearly that users can use internal complaint handling or other settlement mechanisms to challenge the decision if the app developer also qualifies as an online platform and is not a micro or small enterprise.</p>
<p><b>Providers of online platforms are prohibited to use 'dark patterns' (Article 23a)</b></p>	<p>The DSA specifically prohibits providers of online platforms from designing, organising, or operating their online interfaces in a way that deceives, manipulates, or otherwise affects the ability of users to make free and informed decisions. The DSA mentions some practices explicitly, such as giving more prominence to certain choices when asking users for a decision.</p> <p>App developers will have to carefully design and organise their online interfaces and consider that the DSA prohibits the use of dark patterns, which it broadly defines. The European Commission will likely provide additional guidance on certain prohibited practices, such as giving more prominence to certain choices when asking</p>

	users for a decision. Small and micro enterprises are exempted from this obligation.
--	--

**What's next?**

The European Parliament and the Council of the EU have approved the final text of the DSA. We expect it to be published in the Official Journal of the European Union and enter into force 20 days after its publication, as early as October 2022.

The DSA will directly apply in all EU Member States 15 months after entry into force or from 1 January 2024, whichever comes later. However, VLOPs and VLSEs will have to comply with the rules earlier than other intermediaries. More precisely, they need to follow the new law four months after the European Commission has designated them as gatekeepers.

**DSA obligations tiering**

The table below reproduces the full scope of obligations applicable to online intermediaries, hosting services, online platforms, marketplaces, and VLOPs/VLSEs.

DSA Obligations / intermediaries	All intermediary services	Hosting services	Online platforms	Marketplaces	VLOPs/VLSEs
Cooperate with authorities to remove illegal content / provide information (Articles 8/9)	x	x	x	x	x
Establish a point of contact to communicate with authorities and users (Articles 10/10a)	x	x	x	x	x
Appoint a legal representative if no establishment in the EU (Article 11)	x	x	x	x	x
Have clear and readable terms and conditions (Article 12)	x	x	x	x	x
Publish yearly reports on content moderation, <i>except for micro and small enterprises</i> (Article 13)	x	x	x	x	x
Put in place a notice and action mechanism (Article 14)		x	x	x	x
State reasons for any actions to users (Article 15)		x	x	x	x
Notify suspicious criminal offences (Article 15a)		x	x	x	x
Put in place an internal complaint-handling system, <i>except for micro and small enterprises</i> (Article 17)			x	x	x
Allow and inform users of out-of-court dispute settlement possibilities, <i>except for micro and small enterprises</i> (Article 18)			x	x	x

Process trusted flagger notices in priority, <i>except for micro and small enterprises</i> (Article 19)			x	x	x
Put in place measures and protection against misuse, <i>except for micro and small enterprises</i> (Article 20)			x	x	x
Additional transparency reporting obligations, <i>except for micro and small enterprises</i> (Article 23)			x	x	x
Do not use dark patterns to deceive or manipulate users, <i>except for micro and small enterprises</i> (Article 23a)			x	x	x
Provide information on online advertising, <i>except for micro and small enterprises</i> (Article 24)			x	x	x
Be transparent on recommender systems, <i>except for micro and small enterprises</i> (Article 24a)			x	x	x
Put in place measures to protect minors / Do not use profiling to show advertising to minors, <i>except for micro and small enterprises</i> (Article 24b)			x	x	x
Collect relevant information on business traders using the platform (Article 24c/24d)				x	x
Inform users of purchased illegal products (Article 24e)				x	x
Assess and mitigate risks (Article 26/27)					x
Put a crisis response mechanism in place (Article 27a)					x
Conduct independent audits (Article 28)					x
Have at least one recommender system not based on profiling (Article 29)					x
Additional online advertising transparency requirements (Article 30)					x
Allow authorities and researchers to access relevant data (Article 31)					x
Establish a compliance function (Article 32)					x
Additional transparency reporting obligations (Article 33)					x

Pay a supervisory fee to the European Commission (Article 33b)					x
--	--	--	--	--	---