

The Digital Services Act (DSA) – What You Need to Know

Legal Alert
October 28, 2022
Foster Garvey Newsroom

Contact

Eva H. Novick

Related Services

Privacy, Cybersecurity &
Data Protection

The Digital Services Act (“DSA”) was published in the [Official Journal](#) yesterday. It becomes effective on November 16, 2022 and will start being enforced on February 17, 2024.

The DSA aims to protect EU citizens’ fundamental rights online. The DSA’s goal is twofold: (1) ensuring the “proper functioning of the internal market” and (2) ensuring that fundamental rights, such as those ensuring freedom of expression and information, protection of personal data, and non-discrimination, are protected online.

Download our [FAQ Sheet](#) containing answers to key questions about the DSA.

Who is affected?

The DSA only applies to certain “intermediary services” that fit all of the following criteria:

- It must be located in the EU, offer services to a “significant number” of consumers located in the EU, or advertise its services in the EU.
- It must provide a service over the internet upon a specific request by a consumer and for which the consumer pays.
- It must be a “mere conduit” service, which provides a consumer with access to a communication network or transmits information in a communication network; a “caching” service, which temporarily stores information to assist in faster delivery through a communication network; or a “hosting” service, which stores information upon a consumer’s request.

Why is this important?

Companies that offer diverse products and services, such as domain name registration, cloud storage hosting, online marketplaces, and social media platforms, are all “intermediary services.” However, “micro and small” businesses that employ fewer than 250 people and have an annual revenue of less than 50 million euros or an annual balance sheet of less than 43 million euros are, for the most part, excluded from complying with the DSA, while “very large” intermediaries are subject to more stringent requirements than their smaller – but not “micro and small” – counterparts.

What do I need to do?

Unlike the DMA, which provides for enforcement only by the European Commission, the DSA will be enforced by the European Commission and each country, depending on where a company is located and whether it is “very large.” Each country can choose the agency or agencies that will enforce the DSA and must designate a digital services coordinator to ensure coordination within the country as well as with other countries, the European Board for Digital Services and the European Commission. The maximum fine for violating the DMA is 6% of a company’s worldwide revenue.

The DSA repeatedly makes clear that it does not preempt other existing EU or specific country law that may otherwise be applicable. However, enforcement is streamlined.

If my company is an “intermediary service,” what will I need to do to comply with the DSA?

If your company is an intermediary service and meets the other criteria for the DSA to apply, you need to provide a publicly available single point of contact for regulators and customers, publicly explain how content moderation is handled and publicly post reports about content moderation, and notify law enforcement authorities of certain known illegal activity. If your company is not located in the EU, you will also need to designate a legal representative in the EU. Next, you will need to determine if your company is a hosting service and what type of hosting service.

I’ve heard there are different requirements for hosting services, online platforms, and very large online platforms or very large online search engines. Is this true?

Yes. Online platforms such as social media, online marketplaces, and app stores are a subset of hosting services. They need to comply with all of the requirements for hosting services and additional requirements. Very large online platforms (VLOP) and very large online search engines (VLOSE) are determined by the number of active users on their site. They need to comply with online platform obligations and additional obligations.

What are the additional requirements for hosting services?

In addition to complying with the requirements for all intermediary services, hosting services need to provide a means of reporting illegal content and provide information back to the person reporting the illegal content. They also need to explain any decision to restrict content or monetary payments or to suspend or terminate its service or a customer's account.

What are the additional requirements for online platforms?

Online platforms need to comply with all of the requirements for hosting services and a number of other requirements. Online platforms cannot use dark patterns and cannot present advertisements based on profiling special categories of data. Online platforms must also provide real-time information about advertisements posted on their sites, provide information about parameters used in recommender systems, verify information about sellers in their marketplace, and provide information about sellers with the product listing. Online platforms also need to publicly post their average monthly number of active users at least once every six months. There are also requirements for online platforms pertaining to users that are minors and to illegal products or services sold on their site.

What is a very large online platform (VLOP) or very large online search engine (VLOSE)? What does it mean if my company is a VLOP or VLOSE?

To be considered "very large," a platform's average monthly users must be 10% or more of the EU's population (currently 45 million active users). To be considered "very large," a search engine's average monthly users must be 45 million active users. A list of the "very large" platforms will be published in the Official Journal of the European Union. VLOPs and VLOSEs must pay an annual supervisory fee and have enhanced reporting requirements regarding content moderation and risk assessments. They must provide their terms and conditions in the official language of each member state in which they offer their services, along with a concise summary of the main points in the terms and conditions. They must also conduct risk assessments, independent audits, and have a separate and independent compliance unit. Additionally, VLOPs and VLOSEs must provide an option in a recommender system that is not based on profiling and have a publicly available searchable database with information about the advertisements placed on their site.

Additional resources:

Additional information about the DSA's requirements can be found [here](#).

Need help?

Foster Garvey advises businesses and individuals across a broad range of industry sectors on legal issues relating to privacy, cybersecurity and data protection. Our interdisciplinary team works diligently to advise clients on current and emerging issues in this area, including

cybersecurity preparedness, risk assessments and compliance, and related disputes and litigation.

If you have any questions about complying with the DMA, please contact Eva Novick at eva.novick@foster.com.