CLIENT ALERTS & INSIGHTS

EU Moves Forward with Broad Regulations on Online Services that Impose Fines up to 6% of a Company's Annual Gross Revenue

MAY 5, 2022

The proposed Digital Services Act will require online services (including social media platforms, search engines, and marketplaces) to implement policies and procedures aimed at increasing transparency and combatting illegal products and content on online platforms.

First proposed over two years ago in December 2020, the Digital Services Act ("**DSA**") was agreed to late last month. The European Parliament (the EU's legislative arm) came to an agreement in principle with the individual EU Member States to move forward with the process of finalizing the DSA.

According to the EU, the DSA will set forth new accountability and fairness standards that online platforms, social media platforms, and other internet content providers must abide by. The DSA sets forth a spectrum of regulatory obligations that will apply to entities on a varied basis, depending on the entity's size, societal role, and impact on individuals' lives.

Broadly speaking, the DSA will counter the sale of illegal products and services on online marketplaces and will combat illegal and harmful content on online platforms such as social media. The DSA also broadly aims to increase transparency and fairness in online services.

In a similar vein to past comprehensive EU legislation, the DSA gives individuals control through transparency requirements that entities must abide by. New judicial or alternative dispute mechanisms must be implemented to allow individuals to challenge content moderation decisions or seek legal redress for alleged damages caused by an online platform. The DSA will also require a certain amount of transparency into entities' algorithms that are used to recommend content or products (i.e., target) to individuals.

Background and EU Legislative Process

The DSA is a smaller piece of a larger package of laws and regulations that have slowly made their way through the EU legislative process. One piece of that package, the Digital Markets Act ("**DMA**") was already agreed to in March 2022. The DMA focuses on regulating anti-competitive and monopolistic behavior in the technology and online platform (digital and mobile) industries. The DMA is at the forefront of a trend, both globally and in the US, of looking to antitrust legislation as a way to regulate technology companies and online services.

With the principal agreement in place, the DSA will now be taken up in a co-legislative manner. Meaning the individual EU Member States (France, Germany, etc.) must take up and pass the DSA

for full approval by the EU Council, which is made up of representatives from each EU Member state. In tandem, the European Parliament will take up the DSA for approval.

Once the European Parliament and full EU Council approve the DSA, the DSA will be finalized and effective. As proposed, the DSA will take effect on the later of 15 months after it becomes effective, or January 1, 2024.

However, very large online platforms (as defined below) will have a shortened timeline and must comply with the DSA within 4 months of the DSA's effective date.

There is a dearth of details of what might end up in the final version of the DSA, and the final scope and impact of the new law will not be known until the final text is released. However, the EU has provided some insight and general principles that will guide the final text. These insights can help the multitude of entities that must prepare for the DSA.

Spectrum of Applicability

The DSA applies to "digital services," which broadly includes online services. Online services can include online infrastructure, such as search engines; online platforms, such as social media; or an online internet marketplace, to smaller websites.

Additionally, the DSA will apply regardless of where an entity is established. If an entity is an online service that operates in the EU, it must comply with the DSA. However, as mentioned above, the applicability of the specific requirements will depend on the size and impact the service has on an individual's daily life.

There are four categories of online services according to the DSA: (1) intermediary services; (2) hosting services; (3) online platforms; and (4) very large platforms. Each subsequent category of online service is also considered a sub-category of the preceding type of online service, meaning the requirements placed on intermediary services are also placed on hosting services, and so on and so forth.

Intermediary services include those entities that provide network infrastructure, with some examples including internet service providers and domain registrars. Hosting services include cloud and website hosting services. Online Platforms include online marketplaces, app stores, economy platforms, and social media sites. Finally, very large online platforms include those online platforms that serve and reach over 10% (about 45 million) of consumers in the EU.

DSA Requirements

The requirements of the DSA are cumulative and will depend on the size and impact of a given company. While specifics and details are currently lacking, entities can begin preparing for the types of policies and procedures that will be required. The requirements that the EU has outlined for the proposed DSA are broken down below by the specific categories of online services.

1. Intermediary Services

If an entity is considered an intermediary service, it must implement policies and procedures related to the following areas: (1) transparency reporting; (2) terms of service/terms and conditions that account for defined EU fundamental rights; (3) cooperation with national authorities; and (4) accurate

points of contact and contact information, as well as appointed legal representatives, where necessary.

2. Hosting Services

If an entity is considered a hosting service, the entity must comply with the above intermediary service requirements.

Additionally, a hosting service must: (1) report criminal offenses (likely related to the sale of illegal products and services, or the posting of illegal and harmful content); and (2) increase transparency to its consumer base through notice and choice mechanisms that fairly inform the individual consumer.

3. Online Platforms

If an entity is considered an online platform, the entity will need to comply with the above intermediary service and hosting service requirements.

Additionally, an online platform must implement policies and procedures that address: (1) complaint and redress mechanism (that includes both judicial and alternative dispute remedies); (2) the use of "trust flaggers"; (3) abusive notices and counter-notices (e.g., dark patterns); (4) the verifications of third party suppliers on online marketplaces (including through the use of random or spot checks; (5) bans on targeted advertising to children and on target advertising based on special characteristics (e.g., race, ethnicity, political affiliation); and (6) transparent information on targeting and recommendation systems.

Specifically, the obligations imposed related to "trust flaggers" will require online platforms to allow trusted flaggers to submit notices related to illegal content or products and services on the given online platform. For an individual to be considered a "trusted flagger" they must meet certain certification requirements. Certification is only granted to those that: (1) have expertise in detecting, identifying, and notifying supervisory authorities of illegal content; (2) is able to exercise its responsibilities independent from the specific online platform; and (3) can submit notices to the proper authorities in a timely, diligent, and objective manner.

4. Very Large Platforms

Very large platforms are the most regulated sub-category of online services under the DSA. Very large platforms must comply with the requirements set forth for intermediary services, hosting services, and online platforms.

Additionally, very large platforms must: (1) implement risk management and crisis response policies and procedures; (2) conduct internal audits, and have external audits conducted, of the services; (3) implement opt-out mechanisms so individuals can opt out of targeted advertising or user profiling; (4) share data with public authorities and independent researchers; (5) implement internal and external-facing codes of conduct; and (6) cooperate with authorities in response to a crisis.

The transparency and audit requirements set forth for very large platforms will require annual risk assessments to identify any significant risks to the platform's systems and services. The risk assessment must include reviews of the following (1) illegal content, products, and/or services; (2) negative effects on defined EU fundamental rights, especially with respect to privacy, freedom of

expression and information, anti-discrimination, and the rights of children; and (3) manipulation of the services and systems that could result in negative effects on public health, children, civic discourse, the electoral system, and national security.

In addition to the risk assessment, independent external auditors will need to conduct assessments of the services and systems at least once a year. Such auditors will need to produce a written report and very large platforms will need to implement and maintain policies and procedures to remedy any identified issue.

Penalty For Noncompliance

Individual EU Member States will have the freedom to implement the specific rules and procedures for how penalties will be issued under the DSA. In the most recent draft, the DSA called for penalties that are "effective, proportionate and dissuasive" meaning the penalties imposed could be imposed where no direct damages occurred or be in excessive of any direct damages.

As proposed, any entity that violates the DSA can face a penalty up to 6% of its annual revenue.

Looking Forward

Once implemented and effective, the DSA will set the standard for requirements related to fairness, transparency, and responsibility that online services must comply with. Entities that fall within any of the DSA's four categories of in-scope digital services will need to begin investing resources into policies and procedures to address the various topics addressed in the DSA.

The DSA sets out a compliance deadline of January 2024, or 15 months after the DSA's final effective date. This gives a number of entities time to jump-start their compliance efforts.

However, the base compliance deadline is a bit deceptive as a large number of entities will likely fall within the very large platform category. Such entities will only have 4 months post-DSA effective date to come into compliance and cannot afford to final approval of the DSA to jump-start their compliance programs.

As Europe continues to lead the way in regulating entities that operate in the increasingly online world, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.