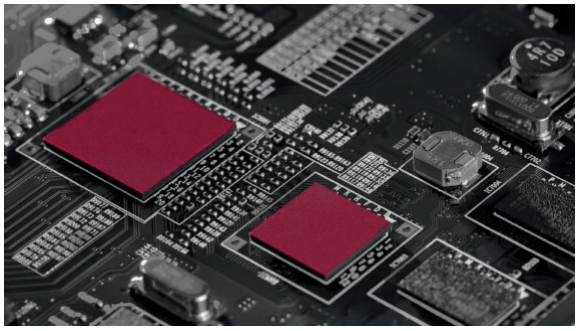
ADVANT Beiten

Tech Law Briefing

July 2022



Digital Services Act ("DSA")

Dear Reader,

The European Parliament and the EU Member States reached a political agreement on the Digital Services Act. The Act aims to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.

Please find below our Tech Law Briefing.

Your Contacts:

Dr Andreas Lober

Email

Cathleen Laitenberger

Email

Lennart Kriebel

Email

Daniel Trunk

Email

Digital Services Act

The European Parliament and the EU Member States reached a political agreement on the Digital Services Act. The Act aims to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.

I. Overview

The Digital Services Act ("DSA") will affect many internet businesses and aims to help brands fighting the sale of copies or fake products or other infringements of their rights on online platforms: the DSA requires online platforms to take action and ensure traders are traceable.

More generally, the DSA regulates online intermediary services, such as hosting services and online platforms, and imposes a long list of obligations on them. Services which allow users to share content will often be qualified as online platforms.

The DSA will also establish a graduated regulatory mechanism. General obligations will apply to all intermediary service providers, while specific obligations are imposed on hosting providers. Online platforms and online marketplaces face wider reaching obligations. Lastly, further obligations will apply to very large online platforms and marketplaces – defined as more than 45 million active users per month in the EU - as well as very large online search engines.

II. Fines

Severe fines of up to six percent of the annual turnover can be imposed for failure to comply with the Act. Member States will generally be responsible for oversight and the imposition of fines. For very large online platforms and very large search engines, the responsibility will lie with the Commission.

"GDPR-style fines of up to 6 % of the total annual turnover will apply to breaches of the DSA."

III. Key points

1. Providers of intermediary services must **act against illegal content** where ordered to do so by the relevant national judicial or administrative authority. Accordingly, the Act requires the intermediary services providers to establish a **single point of contact for direct communication** with the authorities and the Commission, as well as a point of contact enabling the users of the service to communicate directly and rapidly with the services provider.

Additional information will need to be provided in the terms and conditions of the services providers. This will ensure the fundamental rights of users, such as freedom of expression, freedom and pluralism of the media, and other fundamental rights are adequately reflected in the terms and conditions. The information shall cover restrictions on information as well as the policies, procedures and tools used for **content moderation**, as well as the internal procedures for **handling complaints**.

Where the intermediary service is primarily directed at or used by minors, the terms and conditions must explain the conditions for and restrictions on the use of the service in a way minors can understand.

2. Providers of hosting services must implement **notice and action** mechanisms. These must include a **report** function for **illegal content** which is easy for users to access.

If restrictions are imposed on user content or behaviour, the service provider must give a clear and specific statement of reasons for the restrictions to any affected recipient of the service.

If a hosting provider becomes aware of any information that gives rise to the suspicion of a criminal offence involving a threat to the life or safety of a person, the provider must inform the relevant authorities.

3. Online platforms will have further obligations. Online platforms, **such as social networks or online marketplaces**, are defined as providers of hosting services that not only store information provided by the recipients of the service **but also disseminate that information to**

the public at the recipient's request (if this is not just an ancillary feature).

These obligations include the establishment of an internal **complaint procedure and out-of-court dispute resolution.** Additionally, providers of online platforms shall process notices about illegal content from **"trusted flaggers"** without undue delay. **Detailed provisions will specify how to deal with users that frequently provide manifestly illegal content.**

"Services allowing users to share information online may be qualified as online platforms and will have to comply with extensive obligations. Businesses should therefore assess now whether their services are online platforms."

New transparency obligations will apply for advertising on online platforms. Generally, users will need to be provided information about the advertiser and the person who paid for the advertising. Providers using **"recommender systems"** must inform users about the main parameters they use for these recommender systems and what options users have to modify or influence these parameters. This should be detailed in the platform's T&Cs.

Online Platforms must not present advertising based on profiling that uses "sensitive" personal data, as defined in Art. 9 of the GDPR. This may even apply where the user has consented to the processing of their personal data.

Online platforms must not present personalised advertising based on profiling to minors, where they are reasonably certain the user is a minor. Providers of online platforms are not required to collect age data only to prevent the presentation of personalised advertising. However, the prohibition will apply if the user's age is known to the provider for other reasons (which most likely includes cases where the age is known through compliance with youth protection rules or communication with the individual user).

Online platform operators should review functions such as "**recommended for you**" or similar. Such algorithm-based suggestions often process user profiles for the purposes of personalised advertising within the meaning of the Act.

Online platforms accessible to minors must implement **appropriate and proportionate measures to ensure a high level of privacy, safety, and security of the minor.**

The use of "**dark patterns**" is expressly prohibited.

Dark patterns include:

- displaying one or more consent options more prominently when asking the recipient of the service for a decision
- repeatedly asking a recipient of the service to make a choice where such a choice has already been made (nagging)
- urging a recipient to change a setting after the recipient has already made a choice
- making it much more difficult to terminate a service than it was to sign up for it (roach motel design)
- making certain choices more difficult or time-consuming than others
- making it unreasonably difficult to discontinue purchases or sign out from a given online platform
- using default settings that are difficult to change, unreasonably biasing the recipient's decision-making.

The European Commission may issue guidance on specific dark pattern practices.

Where a platform allows consumers to conclude distance contracts with traders, the platform must ensure **traders are traceable**. They must collect specific information about the trader's identity in order to contribute to a safe, trustworthy and transparent online environment for consumers and other interested parties, such as competing traders and intellectual property right owners.

4. Very large online platforms and very large search engines must establish risk management systems and meet specific compliance requirements. They must be publicly accountable for meeting these requirements and will be subject to annual independent audits. Users must be able to reject recommendations based on profiling. They must also provide greater transparency with respect to online advertising. Additional codes of conduct apply as well. In a crisis (such as war), very large online platforms may be subject to further obligations. These requirements also apply to very large search engines.

EDITOR IN CHARGE:
Dr Andreas Lober | Rechtsanwalt
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH

Update Preferences | Forward

Please note

This publication cannot replace consultation with a trained legal professional. If you no longer wish to receive information, you can unsubscribe at any time.

© Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH
All rights reserved 2022

Imprint

This publication is issued by Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No.: DE811218811
For more information see:
www.advant-beiten.com/en/imprint

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH is a member of ADVANT, an association of independent law firms. Each Member Firm is a separate and legally distinct entity, and is liable only for its own acts or omissions.