

# EU DIGITAL SERVICES ACT: FUNDAMENTAL CHANGES FOR ONLINE INTERMEDIARIES?

Date: 4 November 2022

## Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Dr. Ulrike Elteste, Camille J. Scarparo, Dr. Thomas Nietsch, Andreas Müller

On 27 October 2022, the Digital Services Act was published in the *EU Official Journal* as [Regulation \(EU\) 2022/2065](#), with the aim to fully harmonize the rules on the safety of online services and the dissemination of illegal content online. The Digital Services Act will require online intermediaries to amend their terms of service, to better handle complaints, and to increase their transparency, especially with respect to advertising.

## SCOPE OF APPLICABILITY

The Digital Services Act applies to all “intermediary services” offered to recipients in the European Union. Intermediary services are “mere conduit” services (Internet access and other communication service providers), hosting services, and caching services.

Intermediary services that constitute “online search engines” or “online platforms” are subject to specific obligations. Online search engines are services that enable users to input queries and search “in principle” all websites on the Internet or all websites in a specific language. Online platforms are platforms displaying information to the public at the request of their service recipients.

“Very large online platforms” and “very large online search engines” will be subject to especially onerous rules.

## A FIRST WAVE OF TRANSPARENCY OBLIGATIONS APPLYING FROM 17 FEBRUARY 2023

Providers of online platforms and search engines will be required to publish information on the usage of their services (Statement) on their website, with an initial Statement to be published by 17 February 2023 at the latest. Small enterprises will be exempt from this obligation, but they will still need to compile the information to be provided to the EU Commission and a new regulatory body, the “Digital Services Coordinator,” upon request.

Other obligations bearing on companies subject to the Digital Services Act will start to apply on 17 February 2024. However, a notable exception concerns intermediaries designated as “very large online platforms” or “very large online search engines” by the EU Commission:

## “VERY LARGE” ONLINE PLATFORMS AND SEARCH ENGINES: MOST NEW OBLIGATIONS APPLY FOUR MONTHS AFTER DESIGNATION

A platform or search engine is “very large” if it has 45 million active monthly service recipients in the European Union and if the EU Commission takes a decision designating it as such. It is expected that the EU Commission

will make the first of those decisions before the end of this year. Companies so notified will have to comply with most of the following obligations four months after the notification:

“Very large online platforms” and “very large online search engines” will be required to, *inter alia*:

- Have a compliance function having certain specific powers and resources;
- Publish their reports on content moderation;
- Provide the EU Commission with access to data that is reasonably necessary to monitor and assess their compliance with the Digital Services Act;
- Tolerate investigations, which may include inspections of their business premises, business records, and algorithms;
- Pay the EU Commission a supervisory fee;
- Establish a public and searchable online repository of their advertisements and related information;
- Monitor, report on, and mitigate any systemic risks stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services; and
- Obtain annual external audit reports on their compliance with the Digital Services Act.

The EU Commission will be able to impose fines on them for violations of the Digital Services Act amounting to up to 6% of their total worldwide annual turnover.

## AN AMENDED FRAMEWORK FOR THE LIABILITY PRIVILEGE OF ONLINE PROVIDERS

The Digital Services Act restates the rules on the liability privileges for intermediary services in its [Chapter II](#) (Articles 4 to 10, which replace Articles 12 to 15 of the [eCommerce Directive 2000/31/EC](#)). The privileges remain broadly the same. In principle, intermediary services are not liable for third-party content they process, provided they act expeditiously upon receiving notices of illicit content (Immunity), but are not obliged to take preemptive checks. However, the EU legislator has introduced the following clarifications and changes:

### Preemptive Screening Does Not Affect Their Immunity

To enjoy Immunity, a provider of intermediary services must confine itself to providing its service neutrally by a merely technical and automatic processing of the data provided to it by its customers. The provider must refrain from playing an “active role” of such a kind as “to give it knowledge of, or control over,” that data (Court of Justice of the European Union – CJEU, Joined Cases C-236/08 to C-238/08). Under the eCommerce Directive, it was unclear whether providers should be deemed to have assumed responsibility for content—thereby losing Immunity—if they performed voluntary preemptive screening, monitoring, and filtering. The Digital Services Act now clarifies that providers shall not be deemed deprived of their Immunity under the Digital Services Act “solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation.”

## Minimum Requirements for Takedown Orders

Takedown orders by EU member state courts or other competent authorities must fulfill certain minimum requirements. In particular, they must:

- Be limited territorially “to what is strictly necessary to achieve its objective”;
- Contain “clear information enabling the provider to identify and locate the illegal content concerned, such as one or more exact URL and, where necessary, additional information”; and
- Contain information about redress mechanisms available to the provider and to the recipient of the service who provided the content.

In addition, intermediaries subject to a takedown order must now inform the authorities if and when they have given effect to the order.

## The Role of Trusted Flaggers

Providers of online platforms must implement the necessary technical and organizational measures to ensure that notices submitted to them by “trusted flaggers” are given priority and are processed and acted upon without undue delay. Trusted flaggers have demonstrated particular expertise in identifying illegal content and must be independent of any provider of online platforms.

## Information Transparency

Hosting providers must put user-friendly notice and action mechanisms in place.

## Increased Checks on Traders

Providers of online platforms that allow consumers to enter into distance contracts with traders must obtain certain minimum information from traders prior to giving them access to their services and design their interface in such a way that traders comply with their own information obligations.

## Proactive Outreach to Consumers

If providers of online platforms become aware of illegal products or services having been offered on their platform to consumers, they must inform the consumers whose contact details they have of (1) the fact that the product or service is illegal, (2) the identity of the trader, and (3) any relevant means of redress.

## OTHER NOTABLE OBLIGATIONS UNDER THE DIGITAL SERVICES ACT

### Obligations for All Providers of Intermediary Services Include:

- They must designate single points of contact for communication with the authorities and with the recipients of their service;
- In the absence of an establishment in the European Union, they must designate a legal or natural person to act as their legal representative in one of the member states where the provider offers its services. This requirement for a representative is becoming more prevalent following an increasing trend of extraterritorial EU laws, such as the [General Data Protection Regulation 2016/679](#) (GDPR); and
- They must adopt rules on admissible content and content moderation that respect the recipients' fundamental rights and provide annual reports on their content moderation to the authorities.

### Additional Obligations for Providers of Online Platforms Include:

- They must ensure a high level of privacy, safety, and security of minors; in particular, they must not present advertisements to minors based on profiling as defined in the GDPR;
- They must have an internal complaint-handling system;
- They must design and operate their online interface in a way that is not manipulative, deceptive (so-called “dark patterns”), or otherwise impairs users’ ability to make free and informed decisions’
- They must provide clear information on “each specific advertisement presented to each individual recipient,” including “meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters”; and
- They must provide information on any recommender systems in place in their terms and conditions.

## RELATIONSHIP BETWEEN THE DIGITAL SERVICES ACT, OTHER EU LAWS, AND EU MEMBER STATE LAWS

As an EU Regulation, the Digital Services Act is directly applicable in the EU member states. While EU member states will still be able to adopt additional rules, this will be limited to laws that pursue other legitimate public interest objectives than those pursued by the Digital Services Act.

The Digital Services Act only replaces the provisions of the [eCommerce Directive 2000/31/EC](#) dealing with the liability of online intermediaries. The remainder of the eCommerce Directive remains in force, as do other EU laws regulating the online sphere, e.g., copyright laws, consumer protection and product safety laws, and the [Platform to Business Regulation 2019/1150](#), a law regulating terms of service used by online providers for their business customers, which still remains relatively obscure to many businesses it concerns. Privacy laws also remain unaffected, namely the [ePrivacy Directive 2002/58/EC](#) and the [GDPR](#).

“Very large” intermediaries will also be subject to the [Digital Markets Act 2022/1925](#).

K&L Gates is an international law firm with European offices in Brussels, France, Luxembourg, Germany, Italy, and the United Kingdom. Our lawyers regularly advise on technology and media law, privacy law, consumer protection and product safety laws, and antitrust law. Our [Global Data Protection team](#), including each of our European offices, remains available to assist you in preparing your compliance with the Digital Services Act.

## KEY CONTACTS



**CLAUDE-ÉTIENNE ARMINGAUD**  
PARTNER

PARIS  
+33.1.58.44.15.16  
CLAUDE.ARMINGAUD@KLGATES.COM



**DR. ULRIKE ELTESTE**  
COUNSEL

FRANKFURT  
+49.69.945.196.416  
ULRIKE.ELTESTE@KLGATES.COM



**CAMILLE J. SCARPATO**  
ASSOCIATE

PARIS  
+33.1.58.44.15.11  
CAMILLE.SCARPATO@KLGATES.COM



**DR. THOMAS NIETSCH**  
PARTNER

BERLIN  
+49.30.220.029.408  
THOMAS.NIETSCH@KLGATES.COM



**ANDREAS MÜLLER**  
ASSOCIATE

BERLIN  
+49.30.220.029.405  
ANDREAS.MUELLER@KLGATES.COM

---

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.