

INFORMATION, COMMUNICATION & TECHNOLOGY

DIGITAL SERVICES ACT

VdA EXPERTISE



November 2022

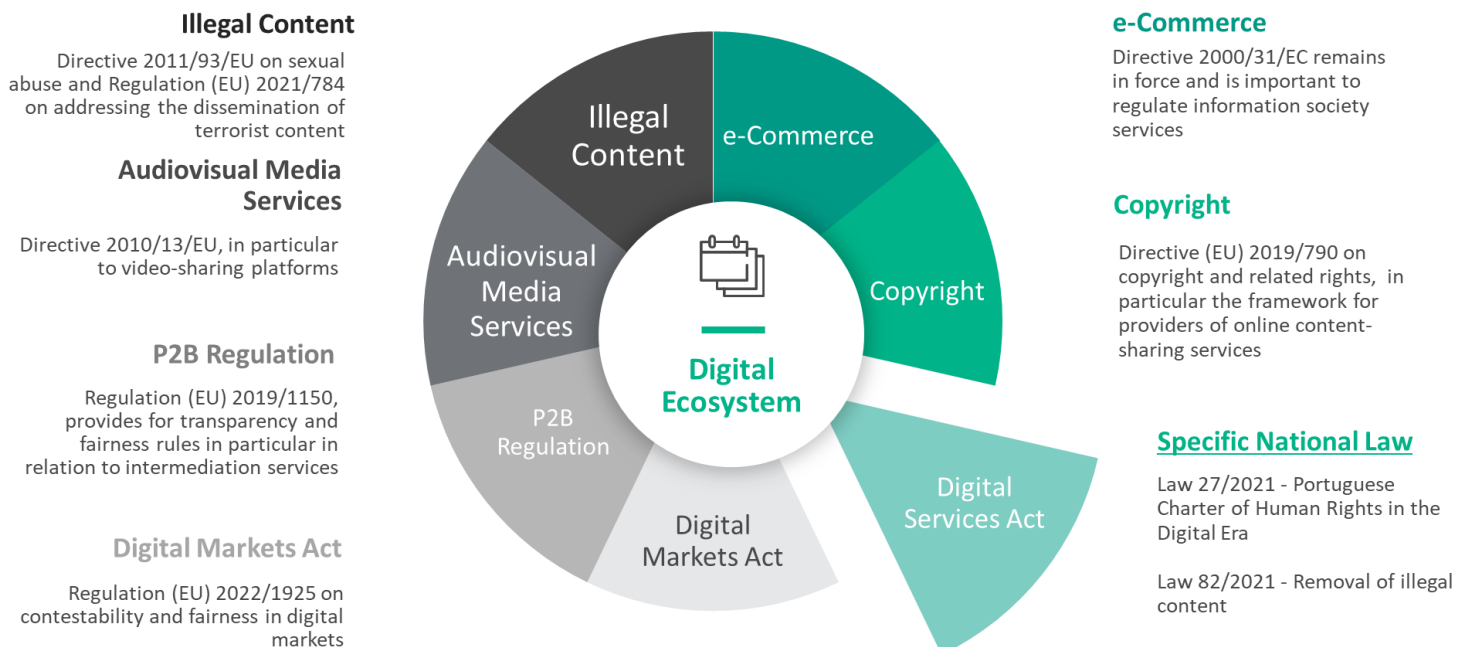
Digital Services Act

The long-awaited **Regulation (EU) 2022/2065 on a single market for digital services ("DSA")**, proposed by the European Commission in December 2020 as part of the Digital Services Act Package, was published on 27 October.

While it is just one piece in a much more complex puzzle (which includes several legislative instruments, as shown in Figure 1), the DSA marks a new era of regulation of the digital ecosystem in the EU. Providers of mere conduit, caching, online search engines and hosting services now have new obligations aimed at increasing users' trust and security in the digital ecosystem.

Moreover, the DSA aims to contribute to a more effective fight against illegal content by revisiting the liability rules of the e-commerce Directive (Directive 2000/31/EC) imposing more appropriate and transparent rules for content moderation, the use of algorithms and the design of online interfaces. It also creates a special and particularly heavy legal framework for very large online platform and search engine providers (without prejudice to the gatekeepers' regime in the DMA).

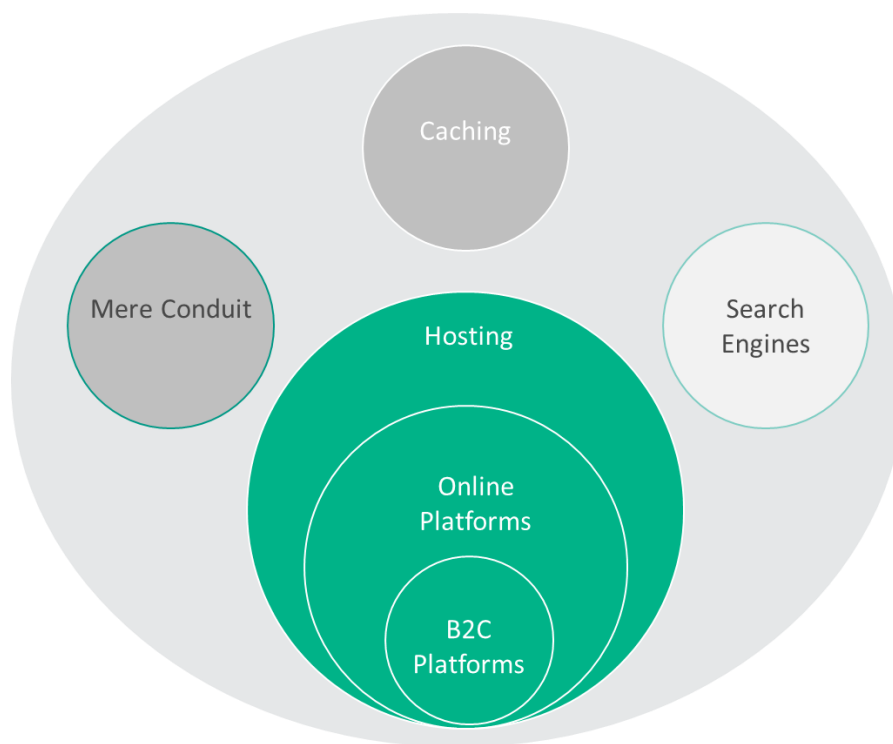
Figure 1 – Example of Laws on the Digital Ecosystem



Accordingly, the responsibilities of the intermediary service providers are clearly defined in the DSA. The obligations are, however, determined according to the different types of providers, based on the nature of their services, their size and their impact on the digital ecosystem, and it is essential to have a clear understanding of their role and framework, as shown in Figure 2.

This document seeks to list some of the most relevant obligations to which the various providers of intermediary services are now subject to.

Figure 2 - Providers of Intermediary Service





"The Digital Services Act is one of the EU's most ground-breaking horizontal regulations and I am convinced it has the potential to become the 'gold standard' for other regulators in the world. By setting new standards for a safer and more accountable online environment, the DSA marks the beginning of a new relationship between online platforms and users and regulators in the European Union and beyond"

Jozef Síkela, Czech Minister for Industry and Trade.

To whom does this apply?

Providers of intermediary services offered to recipients whose place of establishment is within the EU or who are located in the EU, irrespective of where the providers of those services have their place of establishment.

A provider that is not established in the EU will be subject to the DSA rules if it has a significant number of users in one or more of its Member States or if its activities are directed to one or more of its Member States.

What types of providers of intermediary services are included?

- **Providers of mere conduit services** – defined as services that consist of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network. This category includes the following services:
 - i. traffic exchange points,
 - ii. wireless access points,
 - iii. virtual private networks,
 - iv. domain name system ("DNS") services and resolvers,
 - v. top-level domain name registries,
 - vi. registration agents,
 - vii. certificate authorities that issue digital certificates,
 - viii. voiceover IP and other interpersonal communication services.
- **Providers of caching services** – defined as services that consist of the transmission in a communication network of information provided by a recipient of the service, involving the

automatic intermediate and temporary storage of that information, for the sole purpose of increasing the efficiency of the information's onward transmission to other recipients upon their request. Examples of such services are content distribution networks enabling or enhancing the functionality of other intermediary service providers and reverse proxy servers.

- **Providers of hosting services** – which correspond to any service that stores information provided by, and at the request of, a recipient of the service, namely cloud computing infrastructure and server storage services. Within this category are also included **Online Platforms**, which, in addition to storing the information, also disseminate, at the request of the recipient of the service, the information to the public (e.g. online marketplaces, app shops, collaborative economy platforms and social media platforms); and
- **Online search engines** – which allow users to check all Internet sites, or Internet sites in a given language, based on a search on any subject and provide links where information related to the requested content can be found.

And another subcategory:

- **Very large online platforms or search engines** – which correspond to providers whose services have an average monthly number of active recipients of the service in the EU equal to or higher than 45 million, the calculation of which shall be further detailed by the Commission.

Applicable obligations

1. Obligations applicable to all categories of providers of intermediary services

Single point of contact

Establish a single point of contact to enable direct communication, by electronic means, with the competent authorities. In addition, set up a contact point to communicate with service recipients directly, quickly and by electronic means. The information necessary to identify and easily communicate with the contact point must be made available to the public.

Legal representative in the EU with direct responsibility

If the service provider has no establishment in the EU, it must appoint a legal representative. This legal representative must be endowed with the necessary resources to ensure efficient cooperation with the competent authorities. The information necessary to identify and easily communicate with the appointed legal representative must be made available to the public and the legal representative may be held liable for failure to comply with the DSA obligations.

Terms and Conditions and disclosure obligations

Include in the Terms and Conditions ("T&Cs") information about any restrictions imposed on the use of its service, such as (i) tools used for content moderation purposes, (ii) information about the algorithms used and (iii) procedural rules of its internal complaint-handling mechanism. In addition users must be informed of any significant changes to the T&Cs.

Minors

If the services are targeted and offered to minors, the conditions and any restrictions on the use of the service must be described in such a way that minors can understand them.

Annual transparency report

Publish, at least once a year, a clear, easily understandable report on any content moderation they engaged in during the relevant period, which shall include information on the following (i) orders received from Member States' authorities regarding illegal content and provision of information; (ii) the content moderation engaged in at the providers' own initiative, including in particular the use of automated tools and the measures taken to assist those responsible for content moderation; (iii) the complaints received through the internal complaint-handling mechanism; (iv) the use of automated means for content moderation. The report shall be published in machine-readable format and in an easily accessible form.

Orders for action against illegal content and provision of information

Comply with orders issued by national judicial or administrative authorities against illegal content and, where applicable, provide information on certain recipients and, in certain cases, inform the concerned user of the order received.

Applicable obligations

2. Additional obligations applicable to providers of hosting services

Notice and action mechanisms

Put in place mechanisms allowing users to notify providers of the presence of illegal content on their services. These mechanisms should be easily accessible and user-friendly, and allow notifications to be submitted electronically only. These notifications give rise to actual knowledge of the existence of illegal content and hence to a corresponding duty of care on the part of the service provider.

Statement of reasons in case of content restriction

Where applicable (e.g. in case of suspension or termination of accounts) notify the concerned recipients of the service of the decision to remove illegal content and state the reasons for that decision. The notification should also include information on whether the decision was taken on the basis of automated means (e.g. through *machine learning techniques*). In addition, whenever there is a suspicion of a crime involving a threat to the life or safety of persons, the provider must immediately inform the police or judicial authorities.

3. Additional obligations applicable to online platforms

Internal complaint-handling mechanism

Set up an internal system that allows service recipients to challenge decisions to remove illegal content, suspend or terminate the service, suspend or terminate the account or restrict the possibility of monetising the content, and always inform those making the complaint of the decision that was adopted.

Out-of-court dispute settlement

Allow recipients of the service who have submitted notifications of removal of illegal content to access any certified out-of-court dispute settlement body, including for complaints that have not been resolved through the internal complaint-handling mechanism.

Annual transparency report

Include in the annual transparency report, in addition to the information identified above, (i) the number of notifications received under the notice and action mechanism and the categorisation of the type of illegal content concerned; (ii) the number of notifications submitted by trusted flaggers; (iii) any action taken following these notifications; (iv) the number of notifications handled by automated means; (v) average time needed for completing the dispute settlement procedures

Applicable obligations

3. Additional obligations applicable to online platforms

Trusted Flaggers

Collaborate and handle notifications submitted by trusted flaggers as a priority in order to identify and remove illicit content.

Measures and protection against misuse

Suspending, for a reasonable period, recipients of the service who frequently provide manifestly illegal content.

Banning of the so-called *dark patterns*

Not to design, organise or exploit its online interfaces in such a way as to deceive or manipulate recipients of the service or as to distort or impair their ability to make free and informed decisions when using the platform.

Transparency obligations concerning advertisement

Ensure that, if there are advertisements on the platform, the recipients of the service can clearly, concisely and unequivocally recognize them as such, as well as identify the advertiser. Moreover, profiling on the basis of special categories of data, such as data on racial or ethnic origin, political opinions and religious beliefs, etc., is also prohibited.

Recommender systems

Where recommender systems are used (i.e. where a fully or partly automated system is used to suggest specific information to recipients of the service or to prioritise such information), provide, in the T&Cs, information on the use of recommender systems, as well as the parameters used and the options available to users to modify or influence those parameters.

Minors

In the case of platforms targeted to minors, measures should be adopted to ensure a high level of protection of privacy, security and safety of minors. Advertisement using profiling techniques must not be presented to minors.

Where Online Platforms allow the conclusion of distance contracts:

Put in place methods to identify and track traders of products or services on the platform to foster user confidence. The provider must develop the platform in such a way as to enable traders to comply with their obligations to provide pre-contractual information and to ensure product safety. If the service provider becomes aware of the marketing of an illegal product or service, the provider must, where possible, notify the purchaser of this fact.

Applicable obligations

4. Additional obligations applicable in particular to very large online platforms and search engines

Risk assessment

Assess, at least once a year, any significant systemic risks stemming from the functioning of the platform (including algorithmic systems) and the use of its services. Appropriate measures should also be taken to mitigate the risks identified.

Crisis response mechanism

In crisis situations, comply with the measures and decisions to be issued by the Commission, which seek to assess whether and how the operation of the platform contributes, or is likely to contribute, significantly to the worsening of the crisis situation. In this case, the service provider must adopt measures to prevent, eliminate or limit any contribution to the crisis situation. A crisis is considered to have occurred when extraordinary circumstances lead to a threat to safety or public health in the EU.

Independent auditing

Ensure the supervision of the risk management measures adopted by the platforms through annual audits carried out by independent entities.

Recommender systems

Without prejudice to the provision of information regarding the features of the recommender systems, make available at least one version of each of its recommender systems that is not based on profiling.

Additional transparency obligations concerning advertisement

If advertisements are displayed on the platform, make available to the public a repository with information about the content of such advertisements, namely the identification of the advertisers and the periods during which they were displayed.

Other obligations

- Provide the Digital Services Coordinator with access to data needed to monitor and evaluate compliance with the provisions of the DSA;
- Set up an independent internal compliance function, whose task is to monitor compliance with the DSA;
- Publish biannual reports with information on any content moderation undertaken;
- Make the report with the results of the risk assessment available to the Digital Services Coordinator.



Other relevant issues

Illegal content should be understood broadly and should include information relating to illegal content, products, services and activities. Illegal content is considered to be any information that, under applicable law, is either contrary to the law (for example, hate speech, terrorist content and illegal discriminatory content) or is related to illegal activities (for example, child sexual abuse images, non-consensual and illegal sharing of private images, online stalking, selling of counterfeit products, selling of products or services in violation of consumer protection law, etc.).

Notice and action mechanisms facilitate the notification to the service provider regarding a specific piece of information that users consider to constitute illegal content, whereby the service provider can decide whether or not to agree with the assessment and whether to remove the content or block access to it.

Trusted flaggers are entities which have demonstrated expertise in fighting illegal content, are independent from any platform, and have been granted this status by the Digital Services Coordinator in their Member State.

Content moderation corresponds to activities, automated or otherwise, aimed at detecting, identifying and fighting illegal content or information incompatible with the T&Cs, and includes measures that affect the availability, visibility and accessibility of that illegal content or information.

Supervision

Supervision will be carried out by Each Member State (through the Digital Services Coordinators), with the support of the new European Board for Digital Services. For very large online platforms and search engines, the supervision shall be conducted by the European Commission.

An EU-wide cooperation mechanism will be established between the competent national authorities of each Member State, the Commission and the Board.

Fines and Penalty Payments

Fines can amount to up to 6% of worldwide annual turnover for non-compliance with the DSA, and up to 1% for the provision of incorrect, incomplete or misleading information. In addition, compulsory penalty payments of 5% of the average worldwide daily turnover may be levied in order to ensure compliance with the rules on the DSA.

Entry into force

The DSA enters into force on 16 November and applies generally to all providers of intermediary services as from 17 February 2024, without prejudice to some articles being applicable from its effective date, in particular to very large online platforms and search engines.

Contacts



TIAGO BESSA
TCB@VDA.PT



IAKOVINA KINDYLIDI
IMK@VDA.PT



BEATRIZ ASSUNÇÃO RIBEIRO
BEA@VDA.PT