UNDERSTANDING THE DSA: A COMPREHENSIVE GUIDE FOR DIGITAL OPERATORS

FEBRUARY 2024

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

Q&A

What is the Digital Services Act and where does it come from?

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act or DSA) is part of the Digital Services Package, which also includes Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act or DMA).

In both cases, the European Union (EU) is seeking to implement a far-reaching reform of the digital sector through directly applicable acts that do not require transposition by the Member States. The overall aim is to protect citizens and businesses through a fairer and more open digital ecosystem and to update EU law to the changing landscape of digital services, online intermediaries and e-commerce.

Unlike the DMA, the DSA is not directly focused on ensuring open markets for new and disruptive players, nor is it aimed at fighting market capture by large players. Its core is different: to ensure a safe, predictable and reliable online environment (Recital 9 and Article 1), through increased transparency, reporting obligations and accountability for moderation and content removal by intermediary services providers.

The DSA builds on previous self-regulatory efforts, including the EU Code of conduct on countering illegal hate speech online and the 2022 Code of Practice on Disinformation.

This means that the DSA, while complementary to the DMA, focuses more on consumers, recipients of services (end users and business users and others) and parties affected by illegal content being shared, transmitted or stored online.

What are the goals of the DSA?

The main objective of the DSA is to ensure the effectiveness of fundamental rights and consumer protection and to combat the dissemination of illegal content and the social risks of disinformation or other illegal or illicit content (such as gender-based violence).

It focuses mainly on the protection of consumers and recipients of intermediary services while also providing a horizontal framework of conditional exemptions from liability for providers of intermediary services.

In order to comprehensively protect the fundamental rights of online users, it establishes a set of harmonised rules on accountability, reporting obligations and due diligence duties for the detection, flagging, management and possible removal of illegal content.

Does the DSA determine what constitutes illegal content?

The DSA does not determine the unlawfulness of the content, although it provides an approximation of what shall be considered 'illegal content' with reference to national and EU law. In particular, the concept should be broadly defined to cover information about illegal content, products, services and activities such as illegal hate speech or terrorist content and unlawful discriminatory content, or which is illegal under the applicable law in relation to illegal activities. Examples include "the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals." (see Recital 12 and Article 3(h)).

What is the relationship between the DSA and the E-Commerce Directive?

The DSA updates the E-Commerce Directive (Directive 2000/31/EC) without replacing it (Article 2). While it maintains a horizontal framework of conditional exemptions from liability for providers of intermediary services, it now provides for due diligence obligations that are tailored and proportionate to specific categories of providers (according to their role, size and impact on the information ecosystem). In addition, the DSA innovates by clarifying that these exemptions should not cease to apply where intermediary service providers carry out voluntary own-initiative investigations or take measures to comply with the law (Article 7). This includes the so-called "Good Samaritan Principle", inspired by Section 230 of the US Communications Act of 1934. Finally, it is expected that the application of the DSA will lead to greater cooperation and convergence between national authorities.

What is the main timeline of the DSA?

The DSA entered into force on 16 November 2022.

By 17 February 2023 (and at least every six months after), online platform providers provided information on the average monthly active recipients of the service in the Union (Article 24(2)).

The European Commission adopted the first designation decisions on 25 April 2023 (Article 33).

On 21 June 2023, the European Commission adopted an Implementing Regulation (EU) 2023/1201 on detailed arrangements for the conduct of certain proceedings. It lays down rules on the Commission's powers to carry out inspections under Article 69 and to take the necessary follow-up measures in accordance under Article 72, as well as rules on the exercise of the right to be heard and access to the file under Article 79.

EU Member States had until 17 February 2024 to designate national Digital Service Coordinators, which is also the starting date for the application of the DSA, except for providers of very large online platforms (VLOPs) and very large online search engines (VLOSE), *i.e.* those with an average monthly number of active recipients in the Union of 45 million or more (Article 92). They had four months from April 2023 to comply. In Portugal, *Autoridade Nacional de Comunicações* (ANACOM) has been designated as the competent authority and coordinator for digital services, while *Entidade Reguladora para a Comunicação Social* (ERC) is responsible for media and other media content, and *Inspeção-Geral das Atividades Culturais* (IGAC) for copyright and related rights.

What is the subjective scope of the DSA?

Unlike its twin brother, the DSA's subjective scope is broad, as it applies to all intermediary services offered to recipients in the Union, including internet service providers, cloud services, messaging, marketplaces, or social networks (Article 2). Service providers without an establishment in the EU are also covered if they offer their services in the single market. The substantial connection to the Union is based on specific factual criteria (Article 3(e)), such as the number of recipients of the service in relation to the population of the Member State and the targeting of activities at one or more Member States.

The liability of larger online platforms is, however, higher. The most prominent rules apply to VLOPs and VLOSEs, which have a significant societal and economic impact and reach at least 45 million users in the EU (*i.e.* 10% of the population). In contrast, micro and small platforms are exempted from the most of the obligations.

How is the DSA organized?

The DSA is structured in five chapters:

Chapter I sets out the general provisions, including its subject matter and scope (Articles 1 and 2). This first chapter also contains definitions of key terms (Article 3);

Chapter II contains provisions on conditional exemptions from liability for providers of intermediary services. More specifically, it sets out the conditions under which the providers of mere conduit (Article 4), caching (Article 5) and hosting (Article 6) services are exempted from liability for the information they transmit and store:

- The liability exemptions in Chapter II merely determine when and under what circumstances intermediary service providers should not be liable for illegal content provided by service recipients. In other words, this is not a positive basis for determining when a provider can be held liable, as this is determined by the applicable Union or national law;

- The exemptions are conditional and only in certain circumstances. In addition, they vary according to the different nature of 'mere conduit', 'caching" and 'hosting', as well as the different positions and capacities of the service providers. This chapter of the DSA also prohibits the imposition of general surveillance or active fact-finding obligations on providers (Section 8) and an obligation for intermediary service providers to take measures against illegal content (Article 9) and to provide information (Article 10) when ordered to do so by national judicial or administrative authorities;

Chapter III outlines the due diligence obligations for a transparent and safe online environment. These due diligence obligations include notice and action procedures for illegal content and the possibility for recipients of services to challenge content moderation decisions:

- Content moderation (Article 3(t)) is the essential 'core' of these obligations. The chapter is divided into five sections, reflecting the tiered, pyramidal or asymmetric approach of the DSA, as the obligations of intermediary service providers increase with their size and type;

- Thus, there are obligations applicable to all intermediary service providers (Section 1 – Articles 1115) and, in addition to these horizontal obligations, other obligations apply to specific operators;

- Section 2 (Articles 16-18) sets out additional obligations (in addition to those in Section 1) for providers of hosting services, including online platforms;

- Section 3 (Articles 20-28) sets out obligations for providers of online platforms (in addition to those in Sections 1 and 2), with the exception of micro and small enterprises (which have not been designated as VLOPs – Article 19);

- Section 4 contains additional provisions applicable to providers of online platforms enabling consumers to conclude distance contracts with traders (Articles 30-32). Again, unless designated as VLOPs, micro and small enterprises are exempted (Article 29);

- Section 5 sets out obligations for providers of VLOPs and VLOSEs in relation to systemic risk management (Articles 34-43);

- Finally, Section 6 (Articles 44-48) contains horizontal provisions on due diligence obligations;

Chapter IV contains provisions on the application, cooperation and enforcement of the DSA;

Chapter V contains the final provisions (Articles 89-93).

Who will enforce the DSA?

In contrast with the DMA, national authorities are also responsible for monitoring and enforcing the DSA in relation to smaller service providers. For VLOPs and VLOSEs, the Commission has almost exclusive competence (Articles 56, 65-78). In other words, the supervision of intermediary service providers under the DSA is a shared responsibility between the Commission and the authorities designated by the Member States (one or more).

Where more than one national authority is designated, a 'Digital Services Coordinator' will be responsible for all matters relating to the supervision and enforcement of the DSA in that Member State. The Member State must ensure that the roles of the competent authorities and the Digital Service Coordinator are clearly defined and that they cooperate closely and effectively in the performance of their tasks (Articles 49-51).

Due to the decentralised nature of enforcement, rules on coordinated investigations and consistency control mechanisms are prominent. On 18 April 2023, the Commission launched the European Centre for Algorithmic Transparency (ECAT), a first-of-its-kind scientific centre that will assist the Commission and national authorities in the monitoring of the compliance with the DSA.

Trusted flaggers, appointed by the Digital Services Coordinators, will benefit from a priority channel to report illegal content, which will also guide enforcement.

How will the DSA be enforced?

The European Commission and the Digital Services Coordinators will have a number of supervisory and investigative powers, including *i)* the power to request information, *ii)* the power to carry out inspections at the premises of providers, *iii)* the power to take interviews and statements from any natural or legal person, including a member of staff or representative of providers, concerning any information relating to a suspected infringement, and *iv)* the power to record the answers, among others in relation to *v)* interim measures and commitments.

As regards the power to impose fines, the maximum threshold for fines is lower than in the DMA – 6% of the annual worldwide turnover of the intermediary service provider in the preceding financial year.

Article 54 is a specific provision on the right of service recipients to claim compensation for any damage or loss suffered as a result of a breach of obligations by intermediary service providers.

RESPONSIBILITY OF INTERMEDIARY SERVICE PROVIDERS

RESPONSIBILITY EXEMPTIONS (ARTICLES 4-6)

These articles are analogous to Articles 12-14 of the Directive on electronic commerce (2000/31/EC), respectively.

They determine the circumstances in which a service provider cannot be held liable for illegal content provided by the recipient of the service.

They do not prevent a judicial or administrative authority from requiring the provider to prevent or put an end to the offence. See Articles 4(3), 5(2) and 6(4).

Conditions for exemption from liability of intermediary service providers

Mere conduit (Article 4)

TO WHOM DOES IT APPLY?

The Provider of a service of transmission of information, through a communication network. Ex.: Internet access providers, messaging services.

The provider is not liable for the information provided that it (cumulatively):

- Does not initiate the transmission;
- Does not select the receiver of the transmission;
- Does not select or modify the information contained in the transmission.

"Caching" (Article 5)

TO WHOM DOES IT APPLY?

The provider of an information transmission service (which temporarily stores information in order to improve its transmission).

The provider is not liable for the information provided that it (cumulatively):

- Does not modify the information;
- Complies with conditions on access to the information;
- Complies with rules for updating information (industry standards);
- Does not interfere with the legitimate use of technology (industry standards);
- Acts diligently to remove information upon knowing of its removal at source.

Hosting (Article 6)

TO WHOM DOES IT APPLY?

A provider of a storage service for information provided by the recipient of the service.

The provider is not responsible for the information provided that:

- It has no actual knowledge of the illegal activity;
- It is not aware of facts that show illegal activity (as regards claims for damages);
- It acts expeditiously to remove/disable content upon becoming aware of the illegality (see Article 16 DSA);
- In the case of an online platform – Amazon, for example – that allows distance contracts to be concluded with traders, if it does not mislead a consumer about the fact that the product is supplied by a third party (paragraph 3);
- The recipient does not act under the authority/control of the supplier (paragraph 2) – for exmaple, providers with online platforms that determine the price of goods offered by traders (recital 23).

"Good samaritan" (Article 7)

Intermediary service providers retain their liability exemptions even when they proactively take voluntary measures in good faith aimed at *i)* identifying and removing illegal content, or *ii)* complying with EU requirements or national law.

No general obligation of monitoring (Article 8)

There is no general obligation to monitor information or actively seek out facts or circumstances that indicate illegal activity.

Order of national judicial/administrative authorities (Articles 9 and 10)

- Order to adopt measures against illegal content: the provider must inform the authority of any effect given to the order without undue delay.
- Order to provide information on the recipient(s) of the service: the provider must inform the authority of its receipt and any effect given to the order.

DUE DILIGENCE OBLIGATIONS FOR A TRANSPARENT AND SAFE ONLINE ENVIRONMENT

TIER 1:
ALL INTERMEDIARIES

Applicable provisions (Articles 11-15)

Supervision

Duty to Designate:

- A Single point of contact for communication with:
  - Member States' authorities;
  - European Commission;
  - European Board for Digital Services;
  - Recipients of the Service;
- Legal representative (of providers of intermediary services that do not have an establishment in the EU).

DESIGNATION OF A SINGLE POINT OF CONTACT (ARTICLES 11 AND 12)

Entities with whom communication must be ensured	MEMBER STATE AUTHORITIES EUROPEAN COMMISSION EUROPEAN DIGITAL SERVICES COMMITTEE	SERVICE RECIPIENTS
Means of communication	Communication by electronic means	Communication by electronic means
Applicable requirements	Direct communications Disclosure of the information necessary for identification and easy communication with the single point of contact Accessibility and updating of information Specification (subject to the minimum conditions laid down in the regulation) of the official language or languages of the Member States that can be used to communicate with the contact point	Direct and fast communication Possibility of opting for means not exclusively dependent on automated tools Disclosure of the necessary information for easy identification and communication with the single point of contact Accessibility and updating of information Other obligations arising from the e-commerce directive – Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000

DESIGNATION OF A LEGAL REPRESENTATIVE (ARTICLE 13)

Which service providers are obliged to designate a "legal representative"?
Provider of intermediary service which do not have an establishment in the Union but which offer services in the Union.

Method of appointment	Designated in writing
Organisation to be appointed	Natural or legal person
Information on the legal representative to be provided to the Digital Services Coordinator	Name Postal address Email address Telephone number Made publicly available (easily accessible and up-to-date)
Role of the legal representative	"Point of contact" for the competent authorities of the Member States, the Commission and the Committee (in addition to or instead of the provider), to deal with issues relating to: · Receipt; · Fulfilment; and · Enforcement of decisions issued in relation to the DSA.
Powers it should be endowed with	The necessary powers and sufficient resources to ensure efficient and timely co-operation with the authorities
Liability	Possibility of liability for non-compliance with the DSA (liability and legal actions that may be brought against the provider)

Equitable design (Article 14)

- Duty to include information in their terms and conditions on any restrictions that they impose in relation to the use of their service (in respect of information provided by the recipients);

- Duty to act in a diligent, objective and proportionate manner in the application and enforcement of such restrictions.

INFORMATION MUST BE

- Set out in clear, plain, intelligible, user-friendly and unambiguous language (in a way that minors can understand when primarily directed to minors or predominantly used by them);

- Made available to the public in an easily-accessible and machine-readable format.

INFORMATION THAT MUST BE INCLUDED IN THE TERMS AND CONDITIONS OF USE OF THE SERVICE

Information on any restrictions imposed by the provider of intermediary services in relation to the use of their service in respect of information provided by the recipients of the service.

Including information on:

- Policies, procedures, measures and tools used for the purpose of content moderation, including:

  - algorithmic decision-making; and
  - human analysis;

- Rules of procedure of the providers' internal complaint handling system.

MANNER IN WHICH THE PROVIDER OF INTERMEDIARY SERVICES MUST ACT WHEN APPLYING AND ENFORCING OF RESTRICTIONS TO THE USE OF THE SERVICE IN RESPECT OF INFORMATION PROVIDED BY THE RECIPIENTS (INCLUDING FOR CONTENT MODERATION)

- Diligent;
- Objective; and
- Proportionate.

With due regard to the rights and the legitimate interests of all parties involved (including fundamental rights of the recipients of the service, such as freedom of expression, freedom and pluralism of the media and other fundamental rights and freedoms).

Transparency (Article 15)

Duty to comply with minimum annual transparency reporting.

REPORTING OBLIGATIONS OF THE PROVIDER OF INTERMEDIARY SERVICES

Frequency: annually (at least).

Method of making available: publicly available in a machine-readable format and in an easily accessible manner

Reporting model: the Commission may adopt templates of reports (format, content, other details).

Reference period: the Commission may adopt harmonised reporting periods.

General report content (clear and easily understandable): reporting any content moderation the provider engaged in during the reporting period.

Format and particular report content (applicable to all providers of intermediary services) organised according to a certain required information categorization:

- Number of orders received from Member States' authorities categorised by:
    - the type of illegal content concerned;
    - the Member State issuing the order;
    - the median time needed to inform the authority issuing the order, or any other authority specified in the order, of its receipt; and
    - the median time needed to give effect to the order;
- Information (meaningful and comprehensible) about the content moderation engaged in at the initiative of the provider (including):
    - Use of automated tools;
    - Training and assistance provided to those in charge of content moderation;
    - Number and type of measures taken (affecting the availability, visibility and accessibility of information provided by recipients and their ability to provide information through the service);
    - Other related restrictions of the service categorised by:
        - Type of illegal content or violation of the terms and conditions of the service provider;
        - Detection method; and
        - Type of restriction applied.
- Number of complaints received through the internal complaint-handling systems;
- Any use made of automated means for the purpose of content moderation, detailing:
    - Qualitative description of such means;
    - Specification of their precise purposes;
    - Indicators of the accuracy and possible rate error of automated means used;
    - Any safeguards applied.

TIER 2:
HOSTING SERVICES, INCLUDING ONLINE PLATFORMS

Additional applicable provisions

Flagging system (Article 16)

Implement user-friendly and accessible mechanisms, exclusively through electronic means, allowing any individual or entity to report specific content they believe is illegal on their service.

Ensure their notification mechanisms are designed to enable and facilitate detailed and well-supported reports of illegal content.

Quickly inform the submitter about their decision regarding the reported content, including information on redress options.

Process all received notices in a timely, diligent, non-arbitrary, and objective manner, even when using automated means for processing.

Statement of reasons (Article 17)

Give a clear and specific explanation to affected users for any of the following actions taken because the user's content is deemed illegal or against their terms and conditions:

- Restrictions on content visibility, like removal, disabling access, or demoting;
- Suspension, termination, or restriction of monetary payments;
- Suspension or termination of the service, either partially or fully;
- Suspension or termination of the user's account.

Reporting of serious crimes suspicions to enforcement authorities (Article 18)

Promptly report to the relevant authorities any suspicion of criminal offenses threatening life or safety, providing all pertinent information.

If unsure of the specific Member State involved, providers should notify law enforcement in their establishment location, their legal representative's location, or Europol.

The 'Member State concerned' is defined as where the offense is believed to have happened, is happening, or may occur, or where the suspected offender or victim is based.

ONLINE PLATFORMS

ADDITIONAL PROVISIONS APPLICABLE TO PROVIDERS OF ONLINE PLATFORMS (ARTICLES 19 TO 28)

Exclusion for micro and small enterprises (Article 19)

The provisions in Section 3 do not apply to online platforms that qualify as micro or small enterprises.

However, they do apply to online platforms that have been designated as very large online platforms, even if they are considered micro or small enterprises.

Internal complaint-handling system (Article 20)

Online platforms must provide a free, electronic complaint system for at least six months, enabling users to challenge decisions related to content removal, service suspension, account termination, or monetization restrictions due to alleged illegal content or terms violation.

Online platforms must process complaints through their internal system in a timely and fair manner.

Out-of-court dispute settlement (Article 21)

Users, including notice submitters, affected by decisions of the online platform can select a certified out-of-court body for dispute settlement, including for unresolved internal complaints. Platforms must provide clear, user-friendly information about these out-of-court options on their online interface.

Both parties in online platform disputes must engage in good faith with the selected certified out-of-court dispute settlement body.

Trusted flaggers (Article 22)

Trusted flaggers are recognized by the Digital Services Coordinator in each Member State as entities that:

- Have specialized knowledge and specific skills for the detection, identification and notification of illegal content;
- Are independent of any online platform provider;
- Carry out their activities for the purposes of submitting notices diligently, accurately and objectively.

Platforms are required to implement necessary technical and organizational measures to prioritize and swiftly process notices from trusted flaggers within their area of expertise.

- They must also report to the relevant Digital Services Coordinator any instances where a trusted flagger has submitted a substantial number of inaccurate, imprecise, or unsubstantiated notices.

Content moderation (Article 23)

Online platforms must suspend services, after a warning, to users frequently posting manifestly illegal content, for a reasonable duration.

They must also temporarily suspend, post-warning, processing of notices and complaints from those often submitting unfounded claims.

Suspension decisions must be based on a case-by-case, objective assessment of misuse, considering all relevant information.

Other obligations (Articles 24-28)

Transparency reporting obligations for providers of online platform.

Online interface design and organization that are transparent and non-manipulative, supporting users' free and informed decision-making (no dark patterns).

Advertising transparency and no profiling of sensitive data. The online platforms showing ads must make sure users can clearly and immediately identify each advertisement as such.

Online platforms using recommender systems must clearly describe in their terms and conditions the main parameters of these systems and any user options to modify or influence them.

Online platforms accessible to minors are required to implement suitable measures to ensure a high level of privacy, safety, and security for minors using their service.

ADDITIONAL PROVISIONS APPLICABLE TO PROVIDERS OF ONLINE PLATFORMS ALLOWING CONSUMERS TO CONCLUDE DISTANCE CONTRACTS WITH TRADERS (ARTICLES 29 TO 32)

Exclusion for micro and small enterprises (Article 29)

The provisions of section 4 do not apply to online platforms allowing consumers to conclude distance contracts with traders that qualify as micro or small enterprises.

However, they do apply to online platforms for distance contracts that have been designated as very large online platforms, even if they are considered micro or small enterprises.

Traceability of traders (Article 30)

Online platforms for distance contracts must collect essential information from traders (know your business customer – KYBC), like contact details, identification, and compliance certification, before allowing service promotion to EU consumers.

Platforms are required to verify the accuracy of trader information using official databases or documents.

If any trader information is inaccurate or outdated, platforms must seek corrections and may suspend services until resolved.

Compliance by design (Article 31)

Online platforms for distance contracts must design and organize their interface to help traders fulfill their pre-contractual, compliance, and product safety information obligations.

They should also verify traders' compliance with information requirements before allowing product or service offerings. Post-approval, they must conduct random checks in official databases to ensure these offerings are not illegal.

Right to information (Article 32)

When an online platform enabling distance contracts learns that an illegal product or service was sold to EU consumers, they must inform buyers, if contact details are available, about:

- The illegality of the product or service;
- The trader's identity;
- Available redress options.

This obligation applies to illegal purchases made within six months before the platform became aware of the illegality.

PROVIDERS OF VERY LARGE ONLINE PLATFORMS (VLOPS) AND VERY LARGE ONLINE SEARCH ENGINES (VLOSES)

ADDITIONAL OBLIGATIONS FOR VLOPS AND VLOSES TO MANAGE SYSTEMIC RISKS

Risk assessments (Article 34)

VLOPS and VLOSES must regularly assess systemic risks related to their services, including algorithms, especially before introducing critical features, notably the following:

- Issues related to gender-based violence, public health, minors' protection, physical and mental well-being;
- Spread of illegal content;
- Effects on civic discourse, elections, and public security;
- Impact on fundamental rights as privacy, expression, and non-discrimination.

Mitigation measures (Article 35)

Platforms must adopt reasonable and effective measures to address identified systemic risks.

Examples:

- Implementing child protection measures like parental controls, age verification, and abuse reporting systems;
- Adapting content moderation processes, including for the rapid deletion of content, in particular to allow users to report it;
- Running tests and adapting its algorithmic systems, including its recommendation systems.

Crisis response mechanism and crisis protocol (Articles 36 and 48)

In the event of a crisis, the Commission, following a recommendation from the Board, can require large online platforms or search engines to:

- Evaluate if their services significantly contribute to a serious threat or are likely to do so;
- Identify and implement specific, effective, and proportionate measures to prevent, reduce, or limit their contribution to the identified threat;
- Report to the Commission by a set date or at regular intervals on their assessments, details and effects of the measures taken, and any other related issues as specified in the decision.

Independent audit (Article 37)

VLOPs, VLOSEs shall Providers provide the Digital Services Coordinator of establishment or the Commission, at their reasoned request and within a reasonable period specified in that request, access to data that are necessary to monitor and assess compliance with DSA.

VLOPs, VLOSEs shall diligently identify, analyze and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. That report shall be substantiated, in writing, and shall include, inter alia, at least the following:

- The name, address and the point of contact of the provider of the very large online platform or of the very large online search engine subject to the audit and the period covered;
- A declaration of interests;
- A description of the specific elements audited, and the methodology applied;
- A description and a summary of the main findings drawn from the audit;
- A list of the third parties consulted as part of the audit.

Profiling for recommender systems and advertising repositories (Articles 38 and 39)

ADVERTISING REPOSITORIES

VLOPs and VLOSEs must maintain an ad repository with details like:

- The content of the advert, the name of the person or organisation to whom the advert is presented and who paid for it;
- Active duration of the ad;
- Targeted user groups and main parameters used;
- User-flagged ads;
- Total and Member-State-wise users number reach for targeted groups.

This repository, excluding personal user data, must be accurate, complete, and accessible via a reliable search engine and APIs. It should be maintained for one year post the ad's last display. The Commission may provide guidelines post-public consultation.

PROFILING FOR RECOMMENDER SYSTEMS

Must provide at least one option (for each recommender system) which is not based on profiling.

Voluntary EU codes of conduct (Articles 45-47)

The Commission and the European Committee are tasked with encouraging the development of EU-wide codes of conduct to effectively implement the regulation, focusing on specific illegal content or systemic risks. These codes should:

- Clearly outline participants' objectives;
- Include key performance indicators and reporting duties, proportionate to each participant's size;
- Be regularly monitored and evaluated by the European Committee and Commission, with actions requested in case of systemic non-compliance;
- In situations of systemic risks, the Commission may invite VLOPs, VLOSEs, and other platforms, as well as civil society organizations, to participate in drafting these codes, setting specific commitments and reporting guidelines.

CONTACT US

DIGITAL SERVICES & E-COMMERCE
ML Digital Clusters

DIGITAL TOGETHER,
FIRM FOR TOMORROW.

HEAD OFFICE
LISBOA
Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTUGAL
ANGOLA
MOÇAMBIQUE
CABO VERDE
SINGAPURA

LexMundi
Member

mlgts.pt

M
L

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS