

GARRIGUES

**Practical guide to the
implementation of the
Digital Services Act**

The Digital Services Act (DSA)



We are pleased to present our “**Practical Guide to the implementation of the Digital Services Act**” in which we explain the main new features introduced by this regulation.

The main objective of Regulation EU 2022/2065 on a Single Market for Digital Services (“Digital Services Act” or “DSA”), which amends Directive 2000/31/EC, is to help create a **safe, predictable and trusted online environment in which fundamental rights are protected**.

The DSA focuses on defining a unified framework on the liability of providers of intermediary services (social networks, marketplaces, search engines, etc.), on which it imposes standards of due diligence depending on the type of services they provide and their size.

Our aim is to help both intermediary services providers and content holders make use of this new framework in order to together achieve the removal of illegal content online, without affecting the fundamental rights of citizens and businesses.

To help you read this Guide, each time the letter “**Q**” appears, click on it in order to move through the document and obtain additional information.

Table of Contents

- MODULE A: Which digital services are affected by the DSA?
- MODULE B: Liability system
- MODULE C: Due diligence obligations
- MODULE D: Competent bodies and penalty rules

MODULE A

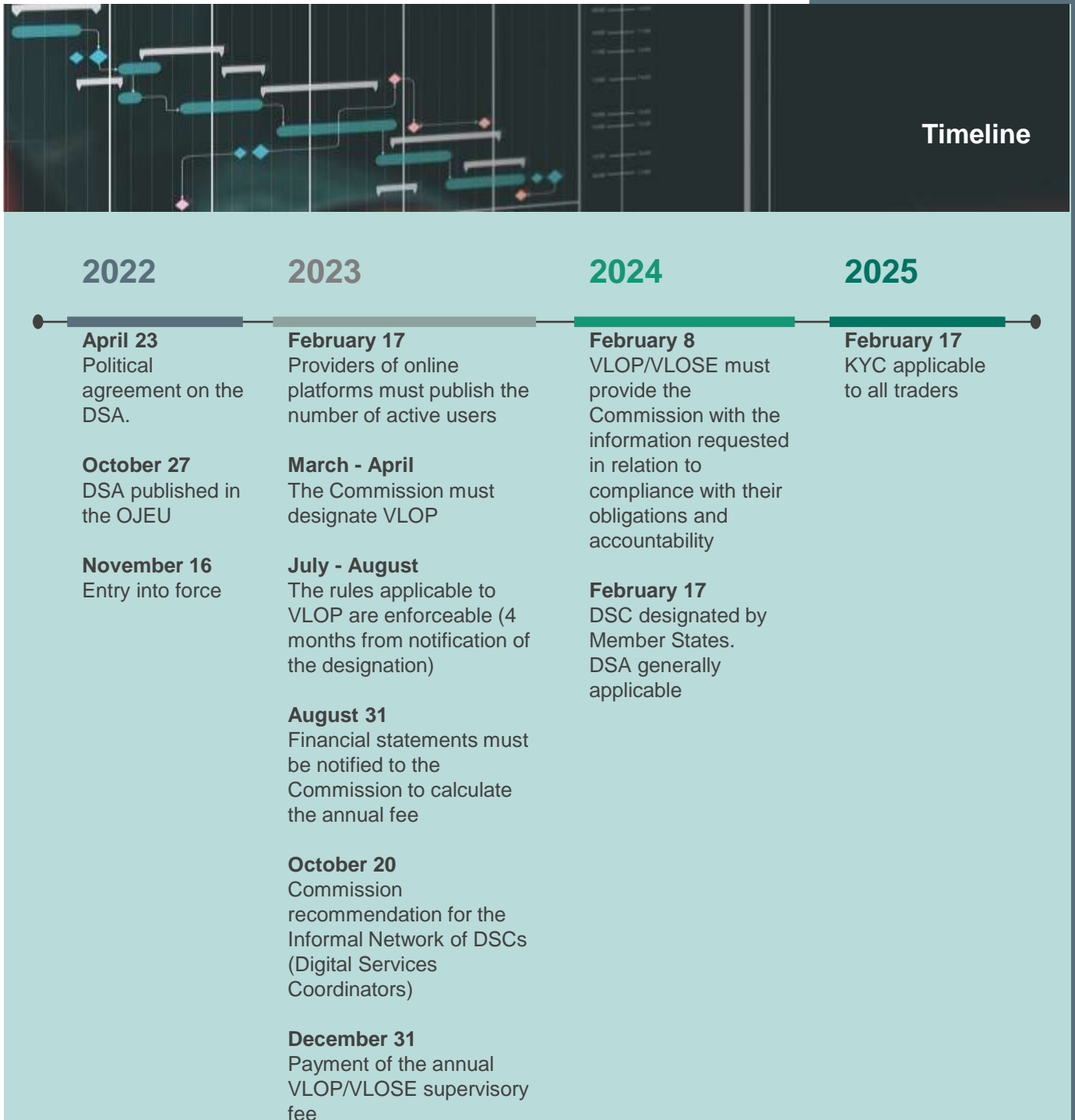
**Which digital services
are affected by the DSA?**

1. When will the Digital Services Act be applicable?

It is already applicable. The DSA will be fully applicable as from February 17, 2024.

Some provisions have been enforceable since August 2023 in relation to certain obligations that affect “very large online platforms” (“VLOP”) and to “very large online search engines” (“VLOSE”) [Q4].

It is a live, complex text complemented by additional rules published by the European Commission to make its application effective.



2. What are the objectives of the Digital Services Act?

The main aim of the DSA is to ensure a safe, predictable and trusted online environment that protects users' rights, while at the same time contributing to the proper functioning of these internal market and facilitating innovation. In other words, **to prevent illegal and harmful activities online and the dissemination of disinformation.**

To achieve this aim, harmonized rules have been established in the following areas:

1

Conditions for the exemption from liability of providers of intermediary services (“**Providers**”) which, in general, adhere to the principles of Electronic Commerce Directive 2000/31/CE [Q6].

2

Progressive transparency and due diligence obligations. This means that greater obligations are imposed on Providers that are closer to users and have a greater number of users [Q34 et seq.].

3

To strengthen the oversight and enforcement of their obligations through the designation of **new oversight and control bodies [Q45]**, as well as the creation of **new penalty rules [Q46]**.



It should be borne in mind that the DSA does not define “*illegal content*”. It depends on the legislation applicable at a national or EU level. This means that there may be differences between the Member States, depending on their internal legislation. In some areas, such as terrorism or child pornography, consensus is widespread. However, other content may generate more doubts, such as hate speech for example.

Where content is illegal in only one State, the general rule is that it should only be removed or access to it disabled, in that particular State, in order to reduce the impact on other fundamental rights.

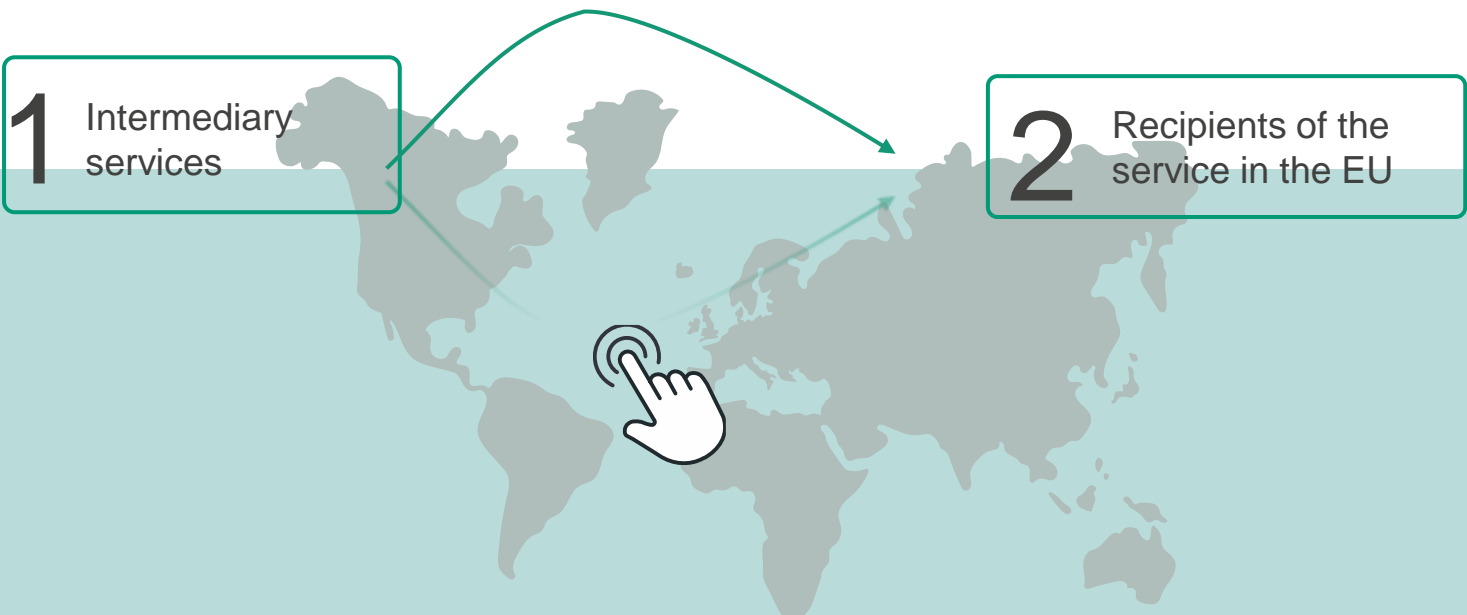
3. What is the territorial scope of the Digital Services Act?

The DSA applies to all Providers with a **substantial connection** to the EU, regardless of where they are located.

When is a **substantial connection** to the EU considered to exist?

- 1 Where the Provider has an establishment in the EU; or
- 2 Where the number of recipients of the service in one or more Member States is significant in relation to the population of that State; or
- 3 Where activities are targeted towards one or more Member States, which is determined based on factors such as the use of a language or a currency generally used in that State, the possibility of ordering products or services in that State (i.e. post code), or the use of top-level domains (i.e. *.es*, *.it*, etc.).

In addition, as is usual in territorial conflicts on the internet **mere technical accessibility to the service** does not establish a sufficiently substantial connection for the DSA to be applicable.



If the Provider does not have an establishment in a Member State but the DSA is applicable for other reasons, it must appoint a **legal representative** [\[Q12\]](#), something many companies already do as part of their obligations arising from other legal instruments.

4. Which services are affected by the DSA? (material scope)

The DSA applies to intermediary services providers, which are divided into three categories depending on the types of intermediation services they provide and their technical functionalities:

“Mere conduit” services

These services are related to network infrastructure, such as internet exchange points, domain name registries, certificate authorities, etc.

“Caching” services

These services store the information temporarily. Content Delivery Network providers fall into this category. They are companies that use caching to store static content from websites in numerous geographic location in order to speed up its delivery to users.

“Hosting” services

These services consist of the storage of information provided by, and at the request of, a recipient of the service, such as cloud computing or web-hosting services. Within these services, the DSA distinguishes between:

- a. **Online platforms:** these services include both storing content and **disseminating it to the public**, so it is not merely storage — provided that such dissemination is not a minor or ancillary feature of the principal service.
- b. **Digital or online markets:** platforms that also enable consumers to conclude distance contracts with traders.
- c. **Search engines:** services that allows users to input queries in order to perform searches.

In addition, platforms and search engines are also classified according to their size. Where they are in excess of 45 million recipients, they are designated as very large online platforms or search engines (“VLOP” and “VLOSE”), with the obligations that this entails.



What does dissemination to the public mean?

That the information is made available to a **potentially unlimited number of persons**, i.e., meaning making the information easily accessible to recipients of the service in general, without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. Accordingly, where access to information requires registration or admittance to a group of recipients of the service, that information should be considered to be disseminated to the public only where recipients of the service seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access.



On April 25, 2023, the European Commission designated 17 online platforms as VLOP and 2 online search engines as VLOSE (click [here](#) for further information). These services had to be adapted within 4 months (August 25, 2023). On December 20, the Commission adopted a second set of decisions and designated a further three online platforms as very large (click [here](#) for further information). On January 18, 2024 the Commission published a summary of the platforms designated and the main control activities (click [here](#) for further information). In addition, decisions are pending on the claims filed by [Zalando](#) and [Amazon](#) at the Court of Justice of the European Union (“**CJEU**”) contesting the classification of their services as VLOP.

5. How is the average monthly active recipients of the service calculated?

To know whether a platform or search engine exceeds the threshold of 45 million users applied by the European Commission to determine whether they are “very large”, it is necessary to look at the “average monthly active recipients” (“AMAR”). It is important to bear in mind that **the AMAR must be calculated for each service individually**, not globally.

When carrying out this calculation it should be borne in mind that the concept “active recipients of the service” is not the same as “recipients of the service”, since it requires a certain degree of engagement with the service, including:



- All the recipients that participate in the service **at least once in a 6-month period**.
- In **multi-sided platforms**, the recipients of all of them are relevant (consumers, professionals).
- **Access from the EU** (concealed locations?).
- **Exposed to information disseminated** on the interface of the online platform (viewing, listening, scrolling over), not just active users.
- **No registration!** Does not coincide with the registered user and it is **not necessary to buy** the product/service.
- **Not equivalent to visits!** They should, as far as possible, be **unique users of the service**.

Once the number of “active” users has been determined, the following AMAR formula can be used:

$$\text{AMAR} = \frac{\text{Unique recipients in the EU} - \text{Visits that are not authentic}}{\text{Number of days in the period}}$$

- The use of different interfaces by the same user (websites or apps), **should only be counted once (deduplicate)**.
- Access from different URLs or domains by the same user (.com, .es or .pt) **should only be counted once (deduplicate)**.
- **Incidental use** by recipients of third-party services must be discounted (**indexing**).
- **Automated users** (*bots*, scrapers) must be discounted.

For further information on identifying and counting active recipients of the service, please see [the Commission’s Guidance on the requirement to publish user numbers](#).

In this site you can confirm the services already designated by the European Commission:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

The Providers themselves must calculate their average AMAR in the last six months and publish it in a section of their online interface that is accessible to the public. However, it is the European Commission that is in charge of designating which providers are VLOP/VLOSE, and it can take into account other data in addition to those provided by the Providers.

MODULE B

Rules on liability

6. What are the rules on liability of providers of intermediary services under the DSA?

This is one of the key questions of the new regulation, since it focuses on determining when the Providers may be responsible for their users' contents.

Generally speaking, the DSA follows the rules on liability of [Electronic Commerce Directive 2000/31/CE](#), which is based on establishing a safe harbor for intermediary services providers to protect them from the consequences of transmitting and/or hosting illegal content of their users.

As a **prior requirement**, the Provider must be an **intermediary**, in the sense that it does not have editorial responsibility for the content. That is, its role with respect to the information provided by its users must be **simply technical, neutral and automatic** (passive).

It is not always easy to determine whether a Provider acts as an intermediary or not, but the DSA gives us some clues. For example, the fact that the Provider automatically indexes information uploaded to its service, offers systems that prevent the identification of the user, has search functions or recommends contents based on the profiles of its users does not give it an active role or affect its safe harbor.

What indicators has the European Commission put in place to determine whether the platform acts as a mere Provider?



Indicator	Provider of the underlying service	Intermediary services provider
Price	Sets the final price	Recommends the final price or gives absolute freedom to choose.
Terms and conditions	Establishes the terms and conditions of the service	Establishes the terms and conditions of use of the platform
Active	Holder of the key assets to provide the service	Assets owned by or under the control of users
Expenses and risks	Defrays the expenses and assumes all the risks	The users providing the services DSA at their own risk
Relationship with the service provider	Employment relationship between the platform and the person who provides the service	Absence of an employment relationship
Quality management	Verification and direct management of the quality of the underlying services	Establishment of rating mechanisms for the evaluation of the service and post sale services

- CJEU [Google France](#) judgment of March 23, 2010 (cases C-236/08 and C-238/08)
- CJEU [eBay](#) judgment of July 12, 2011 (case C-324/09)
- Madrid Appellate Court [Youtube](#) judgment no. 5057/2014, of January 14, 2014
- CJEU [Uber](#) judgment of December 20, 2017 (case C-434/15)
- CJEU [AirBnB](#) judgment of December 19, 2019 (case C-390/18)
- CJEU [Coty v Amazon](#) judgment of April 2, 2020 (case C-567/18)

Once this requirement is met, the conditions for Providers to maintain their exemption from liability depend on the type of service they provide:



“Mere conduit” services

They will not be responsible for the information transmitted if they: (i) do not initiate the transmission; (ii) have not selected the receiver; and (iii) have not selected or modified the information contained in the transmission.



“Caching” services

They will not be liable for the automatic, intermediate and temporary storage of the information transmitted if they: (i) do not modify the information; (ii) comply with conditions on access to the information; (iii) comply with rules regarding the updating of the information; (iv) do not interfere with the lawful use of technology; and (v) act **expeditiously [Q8]** to remove the illegal content when they have **actual knowledge [Q7]** that the information at the initial source of the transmission has been removed from the network; that access to it has been disabled; or that a judicial or an administrative authority has ordered such removal or disablement.



“Hosting” services

They will not be liable for the information stored at the request of recipients if: (i) they do not **have actual knowledge of illegal activity or illegal content [Q7]**; and (ii) if they do, act **expeditiously [Q8]** to remove or to disable access to the illegal content.



The DSA maintains the **prohibition on imposing a general monitoring obligation on platforms** of the contents uploaded by users, which is a cornerstone for the development of digital businesses. That is, these platforms are not under the obligation to verify *ex ante* whether the content uploaded by users is legal.



In the case of digital markets in which the services consist of providing a direct interaction between buyers and sellers, the marketplace must make it clear to users that the product or service in question is provided by a third party **[Q30]**. The aim is not to lead consumers to believe that the service is offered by the platform itself, making it clear at all times who is selling the product in question. If this information and transparency requirement is not met, the marketplace could end up being liable for the content hosted by its users.

7. When do Providers gain “actual knowledge” of illegal activity or content?

Since there is no obligation to supervise the content hosted by users, Providers are not obliged to act against illegal content until they have **actual knowledge** that it is actually illegal.

Determining when this actual knowledge occurs has been one of the most hotly debated issues by the courts in the Member States. It is not always easy to determine when reported content is actually illegal. For example, there is widespread consensus when requests are made to remove videos containing child pornography or blatant fakes. However, this is not true of other contents in which it is not clear that they are illegal such as, for example, contents that breach the right to honor or privacy which could be protected by the right to freedom of expression and information of the person posting the content.

The DSA introduces a very useful tool to determine when actual knowledge takes place, since Providers must be able to determine whether the content is **manifestly illegal without a detailed legal examination**.



Ways in which Providers gain actual knowledge of the existence of illegal content

- Reports by users
- Orders received from competent authorities
- Investigations by the Providers themselves

However, the mere fact that the Provider (i) is aware, generally, that its service is used to store illegal content; (ii) automatically indexes information uploaded to its service; or (iii) has a search function and recommends information based on the profiles or preferences of the recipients of the service, is not sufficient.

Actions following a notification by an authority to remove the illegal content



1

Verification

Verify that the order received (i.e., administrative requests, etc.) meets the minimum requirements, which include:

- Legal ground:** legal provision on which the removal is based.
- Reasoning:** reasons explaining why the content should be removed and the provision on which it is based (i.e., 248 Criminal Code).
- Identification:** of the authority issuing the order (i.e. Madrid Examining Court no. 5)
- Territory:** the order must identify the territory affected (i.e., Spain).
- Location:** clear information on where the illegal content is located (a URL address, reference, etc.)
- Redress:** Providers and the owner of the content affected must be informed of the redress mechanisms available so that they do not have to remove the content.
- Authority:** the order must also indicate which authority is to receive the information about the effect given to the orders. That is, who the Provider must inform of its decision to remove (or not remove) the content in question.

2

Receipt

It must have been received at the single point of contact and in one of the languages that the Provider indicates it is familiar with.

3

Decision

Decide whether it is pertinent to withdraw the content or not.

4

Report

Once the decision has been reached, inform the authority indicated in the order, **without undue delay**, of the effect given to the order to remove the content.


5

Notify the user affected

Inform the user affected by the removal of the content, unless the order prevents this. The user can be informed when the content is removed or when the authority issuing the order says so. The following should be indicated: (i) the reasons, unless the order prohibits this; (ii) the redress available, which will be indicated in the order; and (iii) the territorial scope.

8. What does it mean to act “expeditiously” to remove or disable access to illegal content?

Once the Provider has actual knowledge of the existence of illegal content it can still take advantage of a “safe harbor” if it acts “expeditiously” to remove or disable access to it. The DSA does not define what it means to “act expeditiously”, but it does offer some guidance based on the type of content reported and how urgent it is to take steps. For example:



The [Code of Conduct on countering illegal hate speech online](#) is a joint initiative of IT companies (YouTube, Microsoft, Twitter and Facebook) and the European Commission, which establishes guidelines and obligations for online platforms with the aim of countering the propagation of illegal hate speech online. One of the key aspects is the obligation on platforms to remove illegal content that incites hatred **within 24 hours of receiving a notice**. This measure seeks to address, quickly and efficiently, the presence of damaging content online, encouraging a safe and respectful digital environment.

Other types of illegal content may require longer or shorter time periods to process the notices, depending on the fact, circumstances and types of illegal conduct in question.

1 A quicker response is expected when the reported content may pose a threat to the life or safety of individuals such as for example, in the context of the COVID-19 pandemic and the dissemination of false information.

2 A quicker response is expected in relation to pornographic content, especially where it is related to cyberviolence, in order to protect victims. Such content includes, non-consensual sex or the dissemination of sexual deepfakes.

3 The removal of other content is expected to require longer time periods.

Some other legal provisions do establish recommended time periods to remove certain types of content. For example, the [Code of Conduct on countering illegal hate speech online of 2016](#) establishes an approximate time frame of 24 hours to deal with valid notices that request the removal of this type of content.

9. Should Providers cooperate with the national authorities?

Yes, Providers should cooperate with the national authorities to remove illegal content and/or to facilitate information on their users of the service.

An order that has been validly issued by the competent judicial or administrative authorities is necessary, written in a language that the Provider declares to know, which must contain, at least, the following information:

A reference to the legal basis of the order.

A statement of reasons explaining why the content should be removed or the request for information.

Identification of the authority issuing the order.

Territory affected.

Clear information of where the content is located, such as the URL address or information identifying the recipient of the service.

Possible redress mechanisms available.

Authorities to which the information should be sent.

The order is only binding if the above requirements are met and is limited to the aspects that are strictly necessary to achieve its objective, including its territorial scope.

Providers must decide whether or not to remove the content and if they decide to do so, to inform the authority issuing the order, **without undue delay**, of the effect given to the request for removal.

Providers must also inform the user affected and, if permitted by legislation, inform them of the reasons for the removal, the redress mechanisms available and the territorial scope of the order.

MODULE C

Due diligence obligations

10. Map of due diligence obligations

The DSA is based on stratified rules on liability according to the type of service and size of the provider. Furthermore, the obligations are cumulative. In the table below you can browse through the various due diligence obligations applicable to Providers.

	Art.	Due diligence obligations	Intermediation	Hosting	Platforms	VLOP
[Q11]	11-12	Contact points				
[Q12]	13	Designation of a legal representative				
[Q13]	14	Terms and conditions				
[Q14]	15, 24	Transparency obligations				
[Q15]	16	Notice and Action mechanisms to provide information to users (NTD)				
[Q19]	17	Statement of reasons				
[Q20]	18	Notification of suspicions of criminal offences				
[Q21]	20	Internal complaint-handling system				
[Q21]	21	Out-of-court dispute settlement				
[Q23]	22	Whistleblowing channel for trusted flaggers				
[Q24]	23	Protection measures against misuse of the services				
[Q19]	24	Transparency obligations for platforms				
[Q25]	25	Online interface design and organization				
[Q26]	26	Advertising on online platforms				
[Q28]	27	Transparency of recommender systems				
[Q29]	28	Measures to protect minors				
[Q30]	30	Traceability of traders				
[Q32]	31	Compliance by design				
[Q33]	32	Obligations on information to the consumer on illegal products				
[Q34]	34	Detection, analysis and assessment of systemic risks				
[Q34]	35	Application of mitigating measures				
[Q44]	36, 48	Crisis response mechanisms				
[Q38]	37	Independent auditing				
[Q40]	38	Recommender systems				
[Q40]	39	Additional transparency requirements on online advertising				
[Q41]	40	Data access and scrutiny				
[Q42]	41	Compliance function				
[Q14]	42	Transparency reporting obligations				
[Q43]	45-47	Codes of conduct				

11. How are the contact points established?

Providers must designate a **single contact point** that enables both the authorities (the judicial or administrative authorities, including national authorities, the European Commission and Board for Digital Services) as well as users to contact them easily by electronic means.



The aim is to create an authentic communication channel

- **Sufficient resources** must be used so that communications take place in a timely and efficient manner. Since they are indeterminate legal concepts, we cannot specify, *a priori*, which deadlines will be considered timely, but reasonable means should be used to address the communications bearing in mind their volume.
- All of the replies **cannot be automated**.
- The information must be **easily accessible** and be kept **up to date**.
- An **acknowledgment of receipt** must be permitted (i.e. through an automatic “received” e-mail) via the email provided by the user or authority that has contacted the provider. It is advisable for the user or authority receiving such communication by email to keep a record for evidence purposes.
- The **languages** available for the communications must be indicated. It must be possible to send the communication in, at least, the languages of the EU countries to which the Provider directs its services, meaning all the countries in which the website is available.
- Where **chatbots or similar instant messaging tools** are used, this should be expressly indicated. Although the DSA does not specify how such indication should be made, we believe that the user could be notified through the chatbot itself (i.e. by sending a message at the beginning of the conversation specifying that the recipient of the conversation initiated by the user is an automated tool), or through labels/designs that enable the user to understand that it is interacting with an instant messaging tool (i.e. using a robot icon or design).

12. The obligation on the part of Providers who do not have an establishment in the EU to appoint a legal representative

Providers with establishments in third countries who offer services in the EU must designate a legal representative in one of the Member States where they offer their services and inform the authorities accordingly.



The aim is to facilitate communication with Providers established in third countries

- The legal representatives may be natural or legal persons.
- They must have the necessary powers and resources to cooperate efficiently with the authorities (i.e. the legal representative may not be subject to bankruptcy or insolvency).
- The same legal representative may be mandated by more than one Provider and operate as a contact point.
- The designation must be made in writing.
- Providers must notify their: (i) name; (ii) postal address; (iii) email address; and (iv) telephone number to the Digital Services Coordinator [Q45] of the State where that legal representative resides. The information must be publicly available easily accessible, accurate and kept up to date.

13. Adaptation of the terms and conditions

The DSA seeks transparency in relation to the moderation policies of Providers. It is now a case not only of complying with the applicable law, but also with the rules defined by Providers. The general principle is freedom of contract, so Providers may define the conduct that their users should follow.

All the Providers must **explain and publish their content moderation policies**, using clear, simple language and where applicable, adapted for minors. The content moderation policies must be easily accessible and published in in a machine-readable format.

1

Formal aspects

- Indicate the policies, procedures, measures and content moderation tools (including algorithmic decision-making and human review).
- Explain the internal complaint handling system [\[Q21\]](#).
- Give details of what constitutes inadequate use of the services (i.e. repeatedly publishing illegal content or unfounded complaints) and its consequences: removal of content? suspension of the account? closing of account?
- Provide information on any “significant changes” to the terms and conditions.

2

Material Aspects

- Diligent, objective and proportional application, **bearing in mind the legitimate rights and interests of all the parties**, including the fundamental rights of the recipients of the service (freedom of expression, freedom and pluralism of the media and other fundamental rights and liberties as enshrined in the Charter).

Another recommendation would be for users to accept the terms and conditions and that mechanisms be implemented to keep a record both of the acceptance and content. For example, **qualified timestamp mechanisms** can be used that provide valid evidence of the content.



In the case of VLOP/VLOSE there are additional obligations:

- To provide a clear and accessible summary of the terms and conditions, including the available remedies and redress mechanisms.
- To publish the terms and conditions in the official languages of all the Member States in which they offer their services.

14. Transparency measures

All Providers must publish **annual** reports on their moderation activities:



Authorities

Orders received from the Member States indicating: (i) type of illegal content; (ii) issuing Member State and the (iii) average time needed to inform the authority and give effect to the order.



Own investigations

Measures implemented, including: (i) use of automated tools; (ii) measures adopted to train human resources (i.e. resources for the design and human review of algorithms); (iii) measures adopted that affect the visibility and availability of content, specifying the number and (iv) any other restriction of the services.

Cumulative categorization according to: (i) content contrary to law or the general T&C; (ii) detection method; (iii) restriction applied; and (iv) description of the use of automated means specifying their purpose, rate of error and accuracy.



Notice and Action

Number of N&A received indicating (i) type of illegal content; (ii) number of notices submitted by trusted flaggers; (iii) Actions carried out depending on whether they are contrary to law or the general T&C; (iv) number of N&A handled with only with automated tools; and (v) average time needed to take Action.



Appeal

Number of claims received including: (i) basis for the claims; (ii) decisions adopted; (iii) average decision-making time; and (iv) number of revocations.

Platforms also have additional obligations:



Out-of-court settlement

Number of disputes submitted to out-of-court resolution bodies indicating: (i) the outcome; (ii) the average time necessary to complete the procedure; and (iii) the share of disputes where the Provider implemented the decision.



Suspension of accounts

Number of suspensions imposed for misuse, distinguishing between suspensions imposed due to: (i) providing manifestly illegal content; (ii) the submission of manifestly unfounded notices; and (iii) the submission of manifestly unfounded complaints.

In addition, the reports must be published in a machine-readable format, which is easily accessible and comprehensible. At present, the European Commission has launched a public consultation to define the format that these reports should follow (see [here](#)).

Both online platforms as well as VLOP and VLOSE, must also submit a statement of reasons to the European Commission [\[Q19\]](#) regarding content moderation, for inclusion in the Transparency Database of the DSA, in which the content moderation decisions they take can be tracked almost in real time:



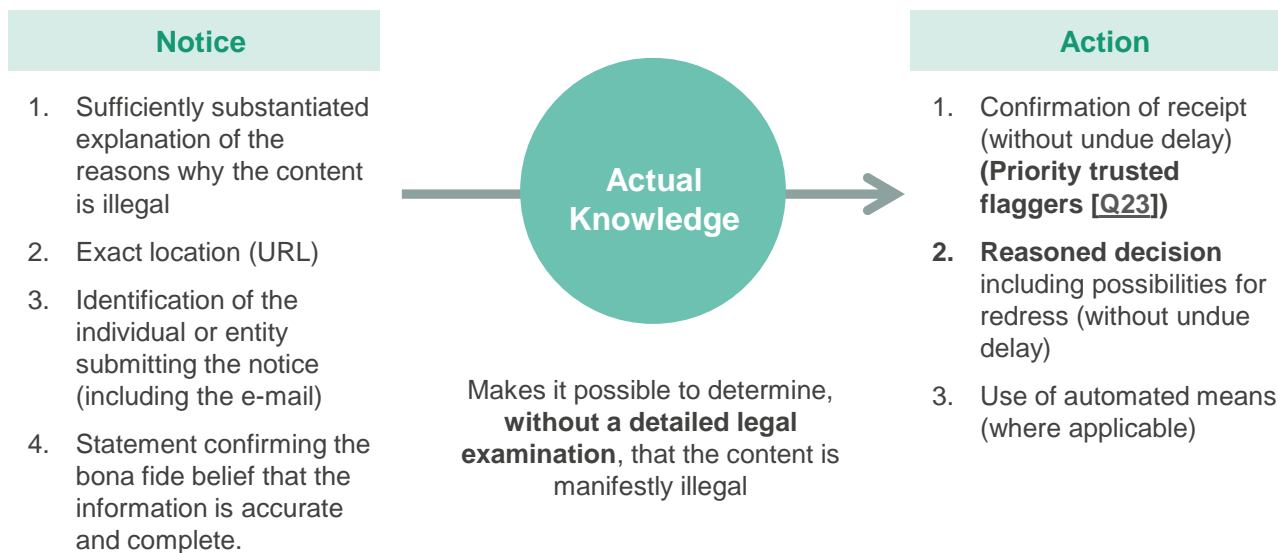
What additional obligations do VLOP and VLOSE have?

VLOP and VLOSE must publish half-yearly reports in one of the official languages of the Member States and must include, apart from the information listed, the following additional information:

- i. The human resources that the platform dedicates to content moderation with respect to the service offered, broken down by each applicable official language.
- ii. The qualifications and linguistic expertise of the persons carrying out the content-moderation activities.
- iii. Indicators of accuracy and related information of the reports broken down by each official language.
- iv. Information on the average monthly recipients of the service for each Member State.

15. What is a notice and action mechanism? (N&A)

Mechanisms that facilitate the notification of illegal content directly to the Providers that host such content. Once the notice is received, if it has been submitted correctly [Q16], Providers are under the obligation to respond [Q17]. This is why they are called notice and action mechanisms.



16. Requirements that the notice forms must meet

In actual fact, to a great extent the DSA reflects the practices that are already in place in the market, mainly influenced by the US, and makes those practices compulsory. Specifically, the forms should be designed to meet the following requirements:

They must be easy to access and user-friendly, and should allow the submission of notices exclusively by electronic means.

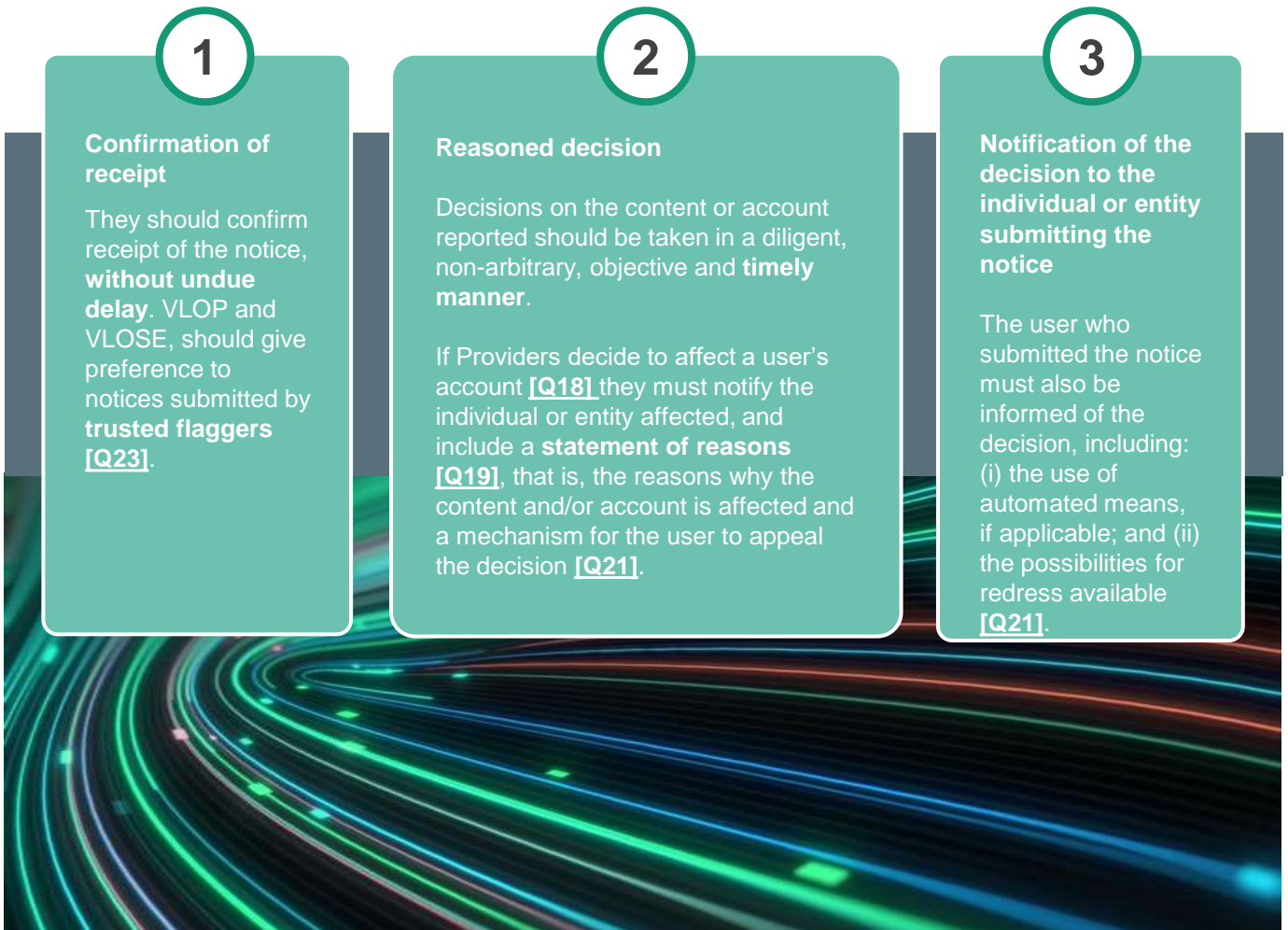
They should contain fields that enable the entity or individual submitting the notice to provide the necessary information, including:

- a sufficiently substantiated explanation of why the content is illegal;
- where the content is located (i.e. URL, reference, etc.);
- the name and email address of the individual or entity submitting the notice
- a statement that they are acting in good faith.

In the description, the individual or entity submitting the notice must be able to notify multiple items of allegedly illegal content through a single notice.

It should allow, but not require, the identification of the individual or the entity submitting a notice (except where their identity is necessary in order to determine whether the information constitutes illegal content). As a result, it should allow users to continue to complete the form if they do not fill in the “Name” and “Surname” boxes.

17. What should the Providers do when they receive a notice?



18. What does “affecting” an account mean?

Providers are considered to be “affecting” an account in any of the following situations:

Restrictions on the visibility of content, including removal of content, disabling access to content, or demoting content.

Impact on the use of means of payment.



Suspension or termination of the service, in whole or in part.

Suspension or termination of the user's account.

19. What is a “statement of reasons”?

The reasons that warrant the Provider suspending an account by, for example, removing certain content.

Minimum content of the statement of reasons:

Reasons

Reasons on which the decision is based, specifying their origin (i.e. notice sent via the notice system or as a result of own investigations).

Grounds

In the case of illegal content, specifying the legal basis and where it is based on incompatibility with the terms and conditions, a reference to the contractual ground relied on.

Automated means

Transparency regarding the automated means used to adopt the decision.

Consequences of the decision

Detailed information on whether the measures to be adopted (i.e. restrictions on visibility, suspension of monetary payments, removal of information) and its duration and territorial scope.

Possibilities for redress

Information on the possibilities for redress available to contest the decision.

There are only **two exceptions** in which it is not compulsory to provide a statement of reasons to affected users: (i) where the individual or entity affected cannot be reached (i.e. the user’s contact details are not known); or (ii) **high-volume commercial content** (disseminated through intentional manipulation of the service, for example bots or fake accounts).



20. What should Providers do if they suspect that a criminal offense is taking place?

In certain cases, Providers may suspect that a criminal offense has taken place or is about to, which involves a threat to the life or safety of persons, be it as a result of its own investigations or notices by third parties. In this case, the provider must notify the law enforcement or judicial authorities without delay.

21. Compulsory mechanisms to contest the decisions taken by Providers

Platforms and VLOP/VLOSE must allow users to contest their decisions [\[Q22\]](#) within six months from the time they were adopted. For this purpose, they must provide internal redress mechanisms, such as information related to the out-of-court dispute settlement.

Internal complaint-handling system



- Recipients of the service may **contest Providers' decisions** where accounts are affected, electronically and free of charge.
- Available for **at least 6 months** from the time the decision was notified
- **AI may not take the decision**; qualified personnel must be used: *Human in the loop!*
- The decision must be notified without undue delay, in a reasoned manner and information must be provided on the possibility of an out-of-court dispute settlement

Certified out-of-court dispute settlement bodies



- The recipient may choose from any of the out-of-court dispute settlement bodies certified by the DSC.
- The decisions are not binding
- Information on this possibility must be provided on the website.
- Payment of the cost by the platform if the out-of-court settlement body agrees with the user.
- Does not affect the possibility of seeking a remedy through the courts.

22. Which decisions can be contested?

The decisions for which redress mechanisms must be provided are the following:

- 1 Decisions whether or not to remove, disable access to or affect the visibility of content.
- 2 Decisions whether or not to suspend or terminate the provision of the service in whole or in part.
- 3 Decisions whether or not to suspend or terminate the user's account.
- 4 Decisions whether or not to suspend, terminate or restrict the ability to monetize information provided by the user.

23. Preference to trusted flaggers

Platforms and VLOP/VLOSE must take the necessary technical and organizational measures to ensure that notices submitted by trusted flaggers are given priority.



Trusted flagger

Trusted flagger status is awarded, following a request in this regard, by the Digital Services Coordinator of the Member State in which the applicant is established, provided that the following conditions are met:

- It must have particular expertise and competence in detecting, identifying and notifying illegal content.
- It must be independent from any Providers
- It must carry out its activities for the purposes of submitting notices diligently, accurately and objectively.

24. New obligations on Providers to actively address the abuse of their services and systems

Providers are under the obligation to protect users from “**misuse**” of their platforms as follows: (i) suspend the accounts of users that **frequently provide manifestly illegal content**; and (ii) suspend the notice and action mechanisms and internal complaints-handling systems of users who make use of them to request the **removal of manifestly unfounded content or to submit manifestly unfounded complaints**.



How should the practice be implemented?

Prior warning

It is compulsory to send a prior warning to the user concerned **before** suspending their account, giving reasons for the suspension and the possibilities of redress against the decision adopted.

Providers must also set out, in a clear and detailed manner, in their terms and conditions, the policy they follow in this regard, and give examples of the facts and circumstances that they take into account when assessing whether certain behavior constitutes misuse and the duration of the suspension.

In addition, Providers may establish stricter measures in their terms and conditions in the case of manifestly illegal content related to serious crimes (i.e. child pornography).

Analysis

Platforms must address each case individually, acting in a diligent, objective and non-arbitrary manner, and taking into account all the facts and circumstances of the case. Before taking protective measures, they must bear in mind: (i) the absolute figures of misuse; (ii) the proportion with respect to the total content; (iii) the gravity of the misuse; and (iv) if possible, the intention of the user affected.

Decision

Where the platform decides to suspend a certain account, it must explain the reasons to the party concerned.

The suspension period must be reasonable (there are no interpretative guidelines).

25. Requirements applicable to the design of the online interface

Platforms and VLOP/VLOSE cannot design, organize or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise distorts or impairs the ability of the recipients of their service to make free and informed decisions (dark patterns).

The European Commission has focused in particular, on practices aimed at prioritizing users' options when they take a decision, insisting that they change a decision already taken or making it difficult to unsubscribe from the service, so that it is more difficult to unsubscribe than to subscribe.



Codes of conduct

The Commission should encourage the drawing-up of voluntary codes of conduct that support and supplement transparency obligations in connection with advertising for providers of online platforms. These codes must establish flexible and effective mechanisms to facilitate and enhance the compliance with those obligations, in particular as concerns the modalities of the transmission of the relevant information on the advertiser and the monetization of data.

The Commission should encourage the preparation of the codes of conduct by February 18, 2025 at the latest and their application by August 18, 2025. Where appropriate, the Commission may invite the Fundamental Rights Agency or the European Data Protection Supervisor to express their opinions on the respective code of conduct.

26. What are the transparency obligations in connection with advertising?

Where a platform, VLOP/VLOSE publishes advertisements on their interfaces, they must fulfill the following obligations:

Identify the information as an "advertisement".

Identify the advertiser and if the advertisement has not been paid by the advertiser, indicate who did.

Facilitate meaningful information 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.

Not present advertisements based on profiling [\[Q27\]](#) using special categories of personal data.

Not present advertisements based on profiling using the user's personal data, when they are aware, with reasonable certainty, that the recipient of the service is a minor.

They must also facilitate certain mechanisms for recipients of the service that is going to present advertising:

Provide a functionality that enables users to declare that certain content is or contains commercial communications.

When a user declares that certain content is commercial, ensure that it is clearly identified as such to other users in real time.

27. What does “profiling” mean?

‘Profiling’ refers to any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

28. New transparency obligations regarding recommender systems

Providers that use recommender systems should describe them in clear and simple language, including: (i) the criteria which are most significant in determining the information suggested to the user; and (ii) the relative importance of those parameters.

In the case of systems that permit several options to offer the information, a functionality should be made available to users to select and modify their preferred option at any time.

The obligation already existed in compliance with [Regulation P2B2C](#) and the [General Consumer and User Protection Law](#).

29. What additional measures should be adopted to protect minors?

Providers that are accessible to minors must:

1 Put in place appropriate and proportionate measures to ensure the privacy, safety, and security of minors.

2 Not present advertisements on their interface based on profiling [\[Q27\]](#) where they are reasonably aware that the recipient of the service is a minor.

These measures do not mean that Providers are obliged to process additional personal data in order to assess whether the recipient of the service is a minor.



30. What obligations are in place in relation to the traceability of traders?

Online markets [\[Q4\]](#) must ensure that traders [\[Q31\]](#) can be traced by users to which they offer their services, and for this purpose must implement the following processes:

1 Obtaining information for the registration of traders

- Name, address, telephone number and email.
- Copy of the identification document.
- Payment account details
- Information from the trade register (if applicable) including the name and registration number.
- Self-certification by the trader undertaking to comply with legislation in the EU.

2 Verification of the information received

Before allowing access to the services, the marketplace must make every effort to verify that the information provided is reliable and complete. Such verification does not have to be very costly. It is suggested that:

- Official online databases and interfaces be used (i.e. national trade registers and the VAT Information Exchange System).
- Trustworthy supporting documents be requested (i.e. certified payment accounts' statements, company certificates and trade register certificates).
- Use other reliable sources.

3 Approval / rejection

Where the platform has reason to believe that certain information is inaccurate, incomplete or not up-to-date, the trader shall be asked to remedy the situation. If it does not do so, the platform should prevent access to the service until the request has been fully complied with.

4 Redress mechanisms

- Mechanisms should be put in place for rejected traders to seek redress.
- Include access to a complaint-handling system and mechanisms for the out-of-court settlement of disputes.

5 Random controls

Aimed at verifying *ex post* on open databases whether the products or services offered have been identified as illegal.

6 Advertising

Part of the information obtained from the offeror should be made available to users on the website interface in a clear, easily accessible and comprehensible manner, including:

- Trader's contact details.
- Details of the register (if it is registered).
- Self-certification of compliance with EU legislation.

7 Storage and confidentiality

The information must be stored in a secure manner for a period of six months from the end of the contractual relationship and be deleted at the end of this period. The information compiled must also be kept confidential, unless a judicial or administrative order specifies otherwise.



In relation to the registration of new traders as from February 17, 2024, this information must be requested before allowing them access. In the case of offerors that were already using the service on this date, this information must be obtained before **February 17, 2025** and if it is not obtained, access to the service must be suspended until the situation is remedied.

31. What is a trader for the purposes of the DSA?

A trader is any natural person, or any legal person irrespective of whether it is privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession

32. Requirements in connection with the design of the interface of online markets

The aim pursued by the DSA is for online markets to allow traders to comply with their obligations regarding pre-contractual information, compliance and product safety. How? By implementing an interface that enables traders to provide, at least, the following information:

- Name, address, telephone number and email address of the economic operator.
- Clear and unambiguous identification of the products or promoted.
- Any sign identifying the trader (i.e. trademark, logo).
- Where applicable, information concerning the labeling and marking in compliance with rules on product safety and compliance.

33. What does the obligation to inform consumers regarding the existence of illegal products or services consist of?

Online markets [\[Q4\]](#) that detect that illegal products or services are being offered on their platform must inform the users that purchased them. Specifically, the following information must be provided:

The fact that the product or service is illegal

The identity of the trader

Any relevant means of redress

Where the contact details of all the consumers affected are not available, said information must be made publicly available in an easily accessible manner on the online interface.

34. What does the requirement that VLOP and VLOSE must analyze the risks of their service consist of?

VLOP and VLOSE must carry out assessments of any systemic risks **[Q35]** stemming from the design, functioning of use of their services, (including the use of algorithmic systems), or from the possible misuse by recipients of the services.

The assessment must bear in mind the severity of the potential impact and probability of such risks (i.e. assess whether the potential negative impact may affect a large number of persons, its potential reversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact). In particular, the following factors must be addressed:

The design of recommender systems and any other algorithmic systems.

The content moderation systems.

The general T&C applicable and their enforcement.

Systems for selecting and presenting advertisements.

Data related practices of the provider.

The intentional manipulation of their service (i.e. creation of false accounts, use of bots or automated exploitation of the service).

The amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with the T&C.



35. What is systemic risk?

Systemic risks are:

Dissemination of illegal content (i.e. dissemination of child sexual abuse) and the performance of illegal activities (i.e. the sale of prohibited products).

Any actual or foreseeable negative effect: (a) on fundamental rights (i.e. misuse of the service through the submission of abusive notices); (b) on civic discourse, electoral processes, and public security; or (c) in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being (i.e. Website the encourages addictions).

36. How often should an assessment of systematic risks be carried?

At least once a year and prior to deploying functionalities that are likely to have a critical impact on the risks identified. The assessment should be stored for three years after they have been performed.

37. Conduct guidelines for platforms in the event that systematic risks are detected

Platforms should implement **reasonable, proportionate** (in light of the Provider's economic capacity and the need to avoid unnecessary restrictions) and **effective** mitigation measures, respecting fundamental rights, focusing in particular on the impact of freedom of expression.

For example, such measures can involve the adaptation of the design and functioning of the services, T&C or content moderation processes, correcting the criteria used in their recommendations, reinforcing internal processes, testing and adapting algorithmic and advertising systems or adjusting cooperation with trusted flaggers.

The following shall also be taken into account:

- 1 the speed and quality of processing of notices.



In this regard, for example, the Code of Conduct on countering illegal hate speech online of 2016, sets a benchmark to process valid notifications for removal of illegal hate speech in less than 24 hours. Other types of illegal content may require longer or shorter time periods to process the notices, depending on the facts, circumstances and types of illegal conduct in question.

- 2 the best interests of minors, especially when their services are aimed at minors or predominantly used by them.

38. How should internal audits be carried out?

VLOP and VLOSE are subject to independent audits [Q39] to assess compliance with their obligations and any supplementary commitments acquired in accordance with codes of conduct and crisis protocols.

It is therefore up to VLOP and VLOSE:

- 1 Provide the necessary cooperation and assistance to the auditors (i.e. giving them access to all relevant data and premises, answering their questions).
- 2 Bear in mind operational recommendations in order to take the necessary measures to implement them and a period of **one month** to adopt an audit implementation report.

39. What is an independent audit vis-à-vis an assessment of systematic risks?

The Regulation requires that these organizations meet the following requirements:

Be independent from the platform (i.e. they have not provided non-audit services related to the matters audited in the prior 12 months, are not performing the audit in return for fees).

Have proven expertise in the area of risk management and technical capabilities to audit algorithms.

Are objective and have professional ethics.

Moreover, the audit report must provide a coherent account of the activities conducted and conclusions reached. The audit reports must provide a clear opinion on the audited service's compliance with the DSA.

Where applicable, the report must include a description of the specific elements that could not be audited and an explanation of why this occurred. It must also include recommendations and measures for improvement that the provider should adopt to comply with the obligations of the DSA. The aim is to try to encourage as much cooperation as possible by those audited.



On October 20, 2023, the Commission adopted a delegated act with the rules applicable to independent audits to assess VLOP and VLOSE compliance with the DSA. The delegated act establishes the steps that the designated services should take to verify the capabilities and independence of their auditor. It also establishes the fundamental principles that auditors should apply when conducting the audits required by the DSA.

Auditors must use templates to prepare the independent audits and the VLOP and VLOSE must also use them to prepare their audit implementation reports. Why? To ensure that the reports on the different services can be compared.

Audits represent an important accountability tool and form part of various transparency requirements of the DSA. The 19 services designated in April 2023 must be submitted to a first audit no later than 16 months after their designation, i.e. at the end of August 2024. They will have to transmit the audit reports to the Commission and the competent authority in the Member State in which they are established and must also publish those reports within three months from the completion of the report on the performance of the audit.

Click [here](#) for further information.

40. Additional transparency requirements for VLOP/VLOSE

VLOP and VLOSE that present advertisements on their interfaces are under the obligation to compile an advertising repository, make it available in a section of their interfaces and ensure that multicriteria queries can be made by means of a search tool. The repository must include exact and complete information on the following matters:



the content of the advertisement (including the name of the product, service or brand and the subject matter of the advertisement).



Name of the advertiser (and, as the case may be, of the person that paid for the advertisement).



Delivery of the advertisement.



Groups of recipients (where applicable) the main parameters used (targeting and delivery criteria).



Commercial communications of the sellers in the marketplaces.



Total number of recipients of the service reached for each Member State (impressions).



It should not contain any personal data of the users of the advertisement.

Recommender systems

VLOP and VLOSE should consistently ensure that recipients of their service enjoy alternative options which are not based on profiling [\[Q27\]](#) for the principal parameters of their recommendation systems. These options should be directly accessible from the online interface on which the recommendations are presented.



European Center for Algorithmic Transparency

On April 18, 2023, the Commission launched the European Centre for Algorithmic Transparency (ECAT), a science center that is a pioneer in its field with headquarters in Seville, which will provide support to the Commission and the national authorities in the supervision of compliance with the DSA.

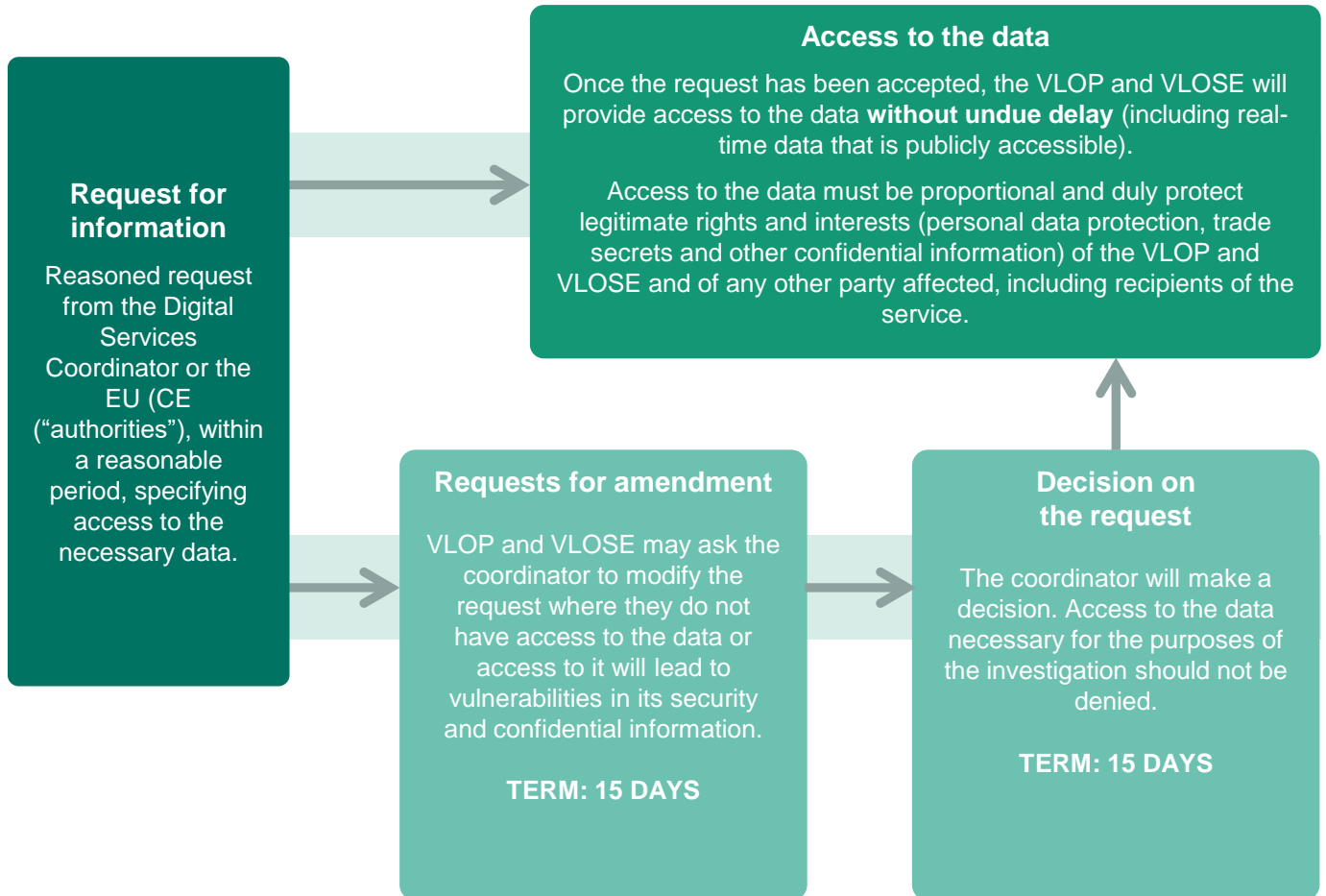
The ECAT will, among other tasks:

- conduct technical tests on algorithmic systems to understand how they work
- analyze transparency reports, risk assessments and independent audits
- provide support to investigations and inspections
- identify emerging risks associated with the use of VLOP/VLOSE
- act as a center of knowledge for research thanks to access to access to the data provided by the DSA.

In this context, the ECAT has also signed a cooperation agreement with the French center Pôle d'expertise de la Régulation Numérique (PEReN), one of the first data science teams in the world that works on matters covered by the DSA. It has also designated the [list](#) of members of the special group on the [EU Code of conduct on age-appropriate design](#), which started its work on June 13, 2023.

41. What data should VLOP/VLOSE share with the public authorities?

In order to monitor and assess compliance by VLOP and VLOSE with their obligations, the Digital Services Coordinator of establishment [\[Q46\]](#) or the Commission may require access to or reporting of specific data, including data related to algorithms.



Use of the data compiled

Monitoring and assessment of the platform's compliance with the DSA, bearing in mind its rights and interests.

Purpose of the request

- **To the authorities:** explanation of the design and functioning of algorithmic and recommender systems.
- **To vetted researchers [\[Q42\]](#):** the data necessary to perform studies to detect systemic risks and assess the measures to mitigate those risks (i.e. data regarding content moderation processes or internal complaint-handling systems, number of views of content by users).



Public consultation on the delegated act regarding access to data

In order to improve the monitoring of the platforms' activities to counter illegal content, as well as other social risks such as the dissemination of disinformation and the risks that may affect users' mental health, vetted researchers are allowed to access certain data of VLOP and VLOSE which had not been disclosed until now.



The consultation on the delegated act took place on **April 25 to May 31, 2023**.



133 contributions were received, which contained information on researchers' need to access data.



Operational issues of the access to data, were addressed, such as the technical requirements and procedure to be followed by data access applications.

Those surveyed underscored the need for a standard request procedure and more guidelines regarding the criteria that researchers need to meet to be vetted. They also highlighted the importance of having a mechanism in place that harmonizes the data access needs of researchers and required greater clarity on the obligations of VLOP/VLOSE.

Based on the contributions received, the Commission is currently preparing a delegated act detailing the technical conditions and procedure that should be followed for effective, practical and clear access to the data that also provides adequate safeguards to prevent abuse. The delegated act is expected to be adopted in the Spring of 2024.

Click [here](#) for further information on the status of the processing of the delegated act.

On January 18, 2024, the Commission sent reasoned requests to the 17 VLOP/VLOSE designated on April 25, 2023, to provide information on the measures they have adopted to comply with their obligations. The platforms must provide that information before February 8, 2024 and following an assessment of the replies received, the Commission will determine whether it should give vetted researchers access to the data. For further information, click [here](#).

42. Requirements to be considered a “vetted researcher”

Researchers that meet the following conditions:

1. that are affiliated to a research organization;
2. that are independent from the standpoint of commercial interests;
3. whose application discloses the funding of the research;
4. who are capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data, and that describe in their request the appropriate technical and organizational measures that they have put in place for this purpose;
5. who demonstrate that their access to the data and the time frames requested are necessary for, and proportionate to, the purposes of their research, and that the expected results of that research will contribute to those purposes;
6. that the research activities envisaged be conducted in order to conduct research that contributes to the detection of systemic risks and the assessment of the suitability, efficiency and risk reduction measures of the VLOP and VLOSE.
7. who have undertaken to make their research results publicly available free of charge, within a reasonable period after the completion of the research.

43. How much importance does the DSA attach to the preparation of codes of conduct by the VLOP/VLOSE?

The Commission and the Board should encourage the preparation of voluntary codes of conduct and the application of the provisions of the codes. The codes will be reviewed and adapted periodically by the Commission and the Board.

Although the implementation of the codes of conduct must be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate.



44. Cooperation obligations of VLOP/VLOSE in crisis situations

In times of crisis, the Commission may require VLOP and VLOSE, on the recommendation of the European Board for Digital Services, to urgently initiate a crisis response.

Specifically, the measures that are considered enforceable are the following:

- A** Assess whether the functioning and use of their services contribute or may contribute to a serious threat.
- B** Identify and apply specific, effective and proportionate measures, to prevent and limit any contribution to the serious threat (i.e. adapting content moderation processes, adapting general conditions, the pertinent algorithmic systems and advertising systems, or adapting the design of their online interfaces).
- C** Inform the Commission of the assessments conducted and of the impact of the measures adopted.



When do we have a “crisis”?

Where extraordinary circumstances exist that may lead to a serious threat to public security or public health in the Union or in significant parts of it. Crises could arise as a result of armed conflicts, including emerging conflicts or acts of terrorism, natural disasters such as earthquakes and hurricanes, as well as pandemics and other serious cross-border threats to public health.

What requirements must the measures that the Commission requires from VLOP and VLOSE meet in crisis situations?

The measures must meet the requirements established in the DSA and be in keeping with the law. Specifically, the Commission must ensure that the following requirements are met:

1. The measures must be strictly necessary, justified and proportionate to the severity of the threat, the urgency and implications for fundamental rights.
2. A reasonable term should be established to adopt them.
3. In principle, the actions should be limited to a maximum period of three months, since they are exceptional.
4. If the crisis evolves, the decision may be revoked, or the application period extended.

The Commission may initiate the drawing up of **voluntary crisis protocols** to coordinate a rapid, collective and cross-border response in the online environment. This may occur for example, where online platforms are misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information.

Given the role played by VLOP/VLOSE in disseminating information they should be encouraged to apply specific crisis protocols, limited to a certain period of time and to address extraordinary circumstances. These protocols do not entail a monitoring obligation nor an obligation to actively seek facts or circumstances indicating illegal activity.

MODULE D

Competent bodies and penalty rules

45. Competent bodies to supervise and enforce the DSA

Digital services coordinator

State level



Exclusive powers over Providers whose main establishment or that of their legal representative is located in the coordinator's territory.

Supervision

Investigation

- Request for information on potential breaches
- Inspection of the Provider's facilities
- Request explanations from personnel

Enforcement

- Accept commitments and make them binding
- Issue cessation orders through judicial authorities
- Fines and periodic penalty payments
- Adoption of interim measures
- Very serious: (1) Action plan; (2) Temporary restriction of access

Trusted flagger certificate

Certificate of out-of-court conflict resolution bodies

European Commission

EU Level



Exclusive powers over VLOP/VLOSE in connection with systemic risks and non-exclusive powers in connection with compliance by VLOP/VLOSE.

- Investigating compliance
- Initiating proceedings
- Requests for information
- Performing interviews and taking statements
- Conducting inspections
- Adopting interim measures
- Negotiating and adopting undertakings
- Monitoring actions
- Breach-related decisions
- Fines and periodic penalty payments
- Access restrictions

European Board for Digital Services

EU Level



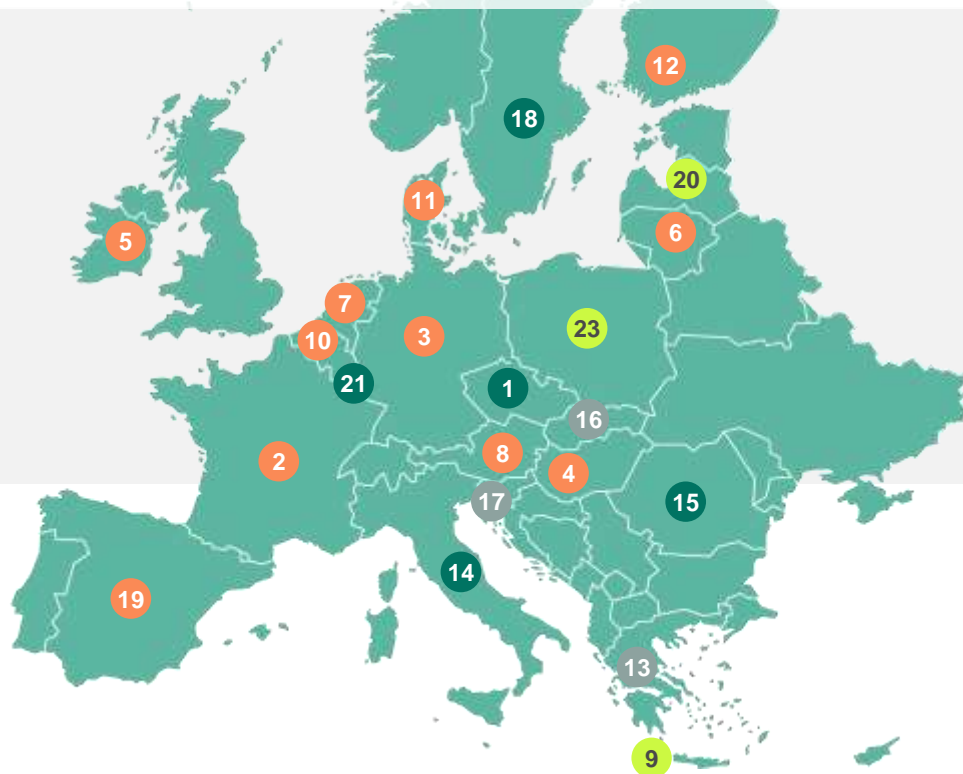
Made up of all the DSCs and headed by the EC.

- Support in the coordination of joint investigations
- Support in the analysis of reports and result of the independent audits applicable to VLOP/VLOSE
- Opinions, recommendations and advice
- Advice to the EC on initiating proceedings against VLOP/VLOSE
- Support, promoting and preparing European rules, guidelines, reports, models and codes of conduct

Progress in the appointment of Digital Services Coordinators

Status

- Executed
- Draft
- Pending information
- Assumption



- | | | |
|---|---|---|
| <p>1 Czech Republic
Czech Telecommunications Office (CTU)</p> | <p>9 Cyprus
Cyprus Radiotelevision Authority (CRTA)</p> | <p>16 Slovakia
Council for Media Services (CMS)</p> |
| <p>2 France
Regulatory Authority for Audiovisual and Digital Communication (ARCOM)</p> | <p>10 Belgium
Flemish Regulator for the Media (Vlaamse Regulator voor de Media).</p> | <p>17 Slovenia
Agency for Communication Networks and Services (AKOS)</p> |
| <p>3 Germany
Federal Network Agency (Bundesnetzagentur)</p> | <p>11 Denmark
Danish Competition and Consumer Authority (Konkurrence- og Forbrugerstyrelsen)</p> | <p>18 Sweden
Post and Telecom Authority (PTS)</p> |
| <p>4 Hungary
The National Media Infocommunications Authority (NMHH)</p> | <p>12 Finland
Finnish Transport and Communications Agency (Traficom)</p> | <p>19 Spain
Spanish Markets and Competition Commission (CNMC)</p> |
| <p>5 Ireland
Ireland's Media Commission (Comisiún na Meán)</p> | <p>13 Greece
Hellenic Telecommunications and Post Commission (EETT)</p> | <p>20 Latvia
Consumer Rights Protection Center (PTAC)</p> |
| <p>6 Lithuania
National Regulatory Authority of the Republic of Lithuania (RRT)</p> | <p>14 Italy
Authority for Communications Guarantees (AGCOM)</p> | <p>21 Luxembourg
Competition Authority</p> |
| <p>7 The Netherlands
Authority for Consumers and Markets (ACM)</p> | <p>15 Romania
National Authority for Management and Regulation in Communications (ANCOM)</p> | <p>22 Malta
Malta Communications Authority (MCA)</p> |
| <p>8 Austria
Austria Communications Authority (KommAustria). Supported by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)</p> | | <p>23 Poland
Office of Electronic Communications (UKE)</p> |

46. And in the event of a breach...

Breaches of the obligations established in the DSA must be punished in an effective, proportionate and dissuasive manner.

Nature, gravity, recurrence and duration

Public interest pursued

Number of recipients of the service affected

Scope and kind of activities carried out

The intentional or negligent nature of the breach

Economic capacity of the infringer

Member States may apply:

- Fines of up to **6% of the worldwide annual turnover** in the event of breach.
- Periodic penalty payments of up to **5% of the average daily worldwide turnover or annual income** of the Provider for each day of delay in payment of the fines.
- Penalties for providing incorrect, incomplete or misleading information, for failing to reply or not rectifying incorrect information and for not submitting to an inspection, with maximum penalties of up to **1% of the annual income or worldwide turnover** of the Provider.

For VLOP and VLOSE, the Commission may impose those penalties where it finds that such provider, intentionally or negligently: a) breaches the relevant provisions of the DSA; b) breaches a decision ordering interim measures; or c) breaches a commitment declared binding through a decision adopted by the Commission.



As a last resort measure, if the infringement continues and causes serious harm to users and involves a criminal offense that threatens the life or safety of individuals, the Commission may request the DSC in the Member State in question to ask the national courts to **temporarily restrict recipients' access to the service**, following a specific procedure.

For further information on these procedures click [here](#).

GARRIGUES

Síguenos



La presente publicación contiene información de carácter general, sin que constituya opinión profesional ni asesoramiento jurídico. © J&A Garrigues, S.L.P., 2024. Quedan reservados todos los derechos. Se prohíbe la explotación, reproducción, distribución, comunicación pública y transformación, total y parcial, de esta obra, sin autorización escrita de J&A Garrigues, S.L.P.

J&A Garrigues, S.L.P. Reg. Merc. Madrid: Tomo 17.456, Folio 186, Sección 8ª, Hoja M-190538.
NIF: B81709081. Hermosilla, 3 – 28001 Madrid, España. + 34 91 514 52 00. info@garrigues.com