Questions and answers on the Digital Services Act*

Brussels, 23 February 2024

Index

1. General information on the Digital Services Act

What is the Digital Services Act?

The Digital Services Act (DSA) regulates the obligations of digital services, including marketplaces, that act as intermediaries in their role of connecting consumers with goods, services, and content.

It better protects users by safeguarding fundamental rights online, establishing a powerful transparency and accountability framework for online platforms and providing a single, uniform framework across the EU.

The European Parliament and Council reached a political agreement on the new rules on 23 April 2022 and the DSA entered into force on 16 November 2022 after being published in the EU Official Journal on 27 October 2022.

The Digital Services Act is a Regulation that is directly applicable across the EU. Some of the obligations for intermediaries include:

- **Measures to counter illegal content online, including illegal goods and services**. The DSA imposes new mechanisms allowing users to flag illegal content online, and for platforms to cooperate with specialised 'trusted flaggers' to identify and remove illegal content;
- **New rules to trace sellers** on online marketplaces, to help build trust and go after scammers more easily; a new obligation **for online marketplaces to randomly check** against existing databases whether products or services on their sites are compliant; sustained efforts to enhance the traceability of products through advanced technological solutions;
- **Effective safeguards for users**, including the possibility to challenge platforms' content moderation decisions based on the obligatory information platforms must now provide to users when their content gets removed or restricted;
- Wide ranging **transparency measures for online platforms**, including better information on terms and conditions, as well as transparency on the algorithms used for recommending content or products to users;
- New obligations for **the protection of minors on any platform in the EU**;
- **Obligations for very large online platforms and search engines** to prevent abuse of their systems by taking risk-based action, including oversight through independent audits of their risk management measures. Platforms must mitigate against risks such as **disinformation or election manipulation**, **cyber violence against women, or harms to minors online**. These measures must be carefully balanced against restrictions of freedom of expression, and are subject to independent audits;
- A new **crisis response mechanism** in cases of serious threat for public health and security crises, such as a pandemic or a war;
- **Bans on targeted advertising on online platforms** by profiling children or based on special

categories of personal data such as ethnicity, political views or sexual orientation;

- **Enhanced transparency** for all advertising on online platforms and influencers' commercial communications;
- A ban on using so-called **'dark patterns'** on the interface of online platforms, referring to misleading tricks that manipulate users into choices they do not intend to make;
- **New provisions to allow access to data to researchers** of key platforms, in order to scrutinise how platforms work and how online risks evolve;
- **Users have new rights**, including a right to complain to the platform, seek out-of-court settlements, complain to their national authority in their own language, or seek compensation for breaches of the rules. Now, representative organisations are able to defend user rights for large scale breaches of the law;
- **A unique oversight structure. The Commission is the primary regulator** for very large online platforms and very large online search engines (reaching at least 45 million users), while other platforms and search engines will be under the supervision of Member States where they are established. The Commission will have enforcement powers similar to those it has under anti- trust proceedings. An EU-wide cooperation mechanism is currently being established between national regulators and the Commission;
- **The liability rules for intermediaries have been reconfirmed and updated** by the co-legislator, including a Europe-wide prohibition of generalised monitoring obligations.

Does the Digital Services Act define what is illegal online?

No. The rules in the DSA set out EU-wide rules that cover detection, flagging and removal of illegal content, as well as a new risk assessment framework for very large online platforms and search engines on how illegal content spreads on their service.

What constitutes illegal content is defined in other laws either at EU level or at national level – for example terrorist content or child sexual abuse material or illegal hate speech is defined at EU level. Where a content is illegal only in a given Member State, as a general rule it should only be removed in the territory where it is illegal.

What rules preceded the Digital Services Act, and why did they have to be updated?

The e-Commerce Directive, adopted in 2000, has been the main legal framework for the provision of digital services in the EU. It is a horizontal legal framework that has been the cornerstone for regulating digital services in the European single market.

Much has changed in more than 20 years and the rules needed to be upgraded. Online platforms have created significant benefits for consumers and innovation, and have facilitated cross-border trading within and outside the Union and opened new opportunities to a variety of European businesses and traders. At the same time, they are abused for disseminating illegal content, or selling illegal goods or services online. Some very large players have emerged as quasi-public spaces for information sharing and online trade. They pose particular risks for users' rights, information flows and public participation. In addition, the e-Commerce Directive did not specify any cooperation mechanism between authorities. The "Country of Origin" principle meant that the supervision was entrusted to the country of establishment.

The Digital Services Act builds on the rules of the e-Commerce Directive, and addresses the particular issues emerging around online intermediaries. Member States have regulated these services differently, creating barriers for smaller companies looking to expand and scale up across the EU and resulting in different levels of protection for European citizens.

With the Digital Services Act, unnecessary legal burdens due to different laws were lifted, fostering a better environment for innovation, growth and competitiveness, and facilitating the scaling up of smaller platforms, SMEs and start-ups. At the same time, it equally protects all users in the EU, both as regards their safety from illegal goods, content or services, and as regards their fundamental rights.

What is the relevance of the Regulation of intermediaries at global level?

The DSA is an important step in defending European values in the online space. It respects international human rights norms, and helps better protect democracy, equality and the rule of law.

The DSA sets high standards for effective intervention, for due process and the protection of fundamental rights online; it preserves a balanced approach to the liability of intermediaries, and establishes effective measures for tackling illegal content and societal risks online. In doing so, the DSA aims at setting a benchmark for a regulatory approach to online intermediaries also at the

global level.

Do these rules apply to companies outside of the EU?

They apply in the EU single market, without discrimination, including to those online intermediaries established outside of the European Union that offer their services in the single market. When not established in the EU, they have to appoint a legal representative, as many companies already do as part of their obligations in other legal instruments. At the same time, online intermediaries also benefit from the legal clarity of the liability exemptions and from a single set of rules when providing their services in the EU.

2. Impact on users

How do citizens benefit from the new rules?

Online platforms play an increasingly important role in the daily lives of Europeans. The rules create a safer online experience for citizens to freely express their ideas, communicate and shop online, by reducing their exposure to illegal activities and dangerous goods and ensuring the protection of fundamental rights. The benefits include:

- **Better services for consumers**: Online marketplaces must identify their business users and clarify who is selling a product or offering a service; this helps track down rogue traders and protects online shoppers against illegal products, such as counterfeit and dangerous products. Online marketplaces are required to inform consumers who purchased a product or service when they become aware of the illegality of such products or services, about a) the illegality, b) the identity of the trader and c) any relevant means of redress. They must randomly check the documentation of products sold on their platform, and should increasingly rely on enhanced product traceability solutions, to make sure fewer and fewer non-compliant goods reach European consumers.
- **New rights for users**: At the same time, citizens can notify illegal content, including products, that they encounter and contest the decisions made by online platforms when their content is removed: platforms are obliged to notify them of any decision taken, of the reason to take that decision and to provide for a mechanism to contest the decision.
- **More transparency on advertising**: Users also receive more information about ads they are seeing on online platforms – for example, if and why an ad targets them specifically. Platforms can no longer present behaviourally targeted ads for minors, nor can they present ads to their users based on profiling that rests on special categories of personal data, such as their ethnicity, political views or sexual orientation.
- **More responsibilities for very large platforms**: Specific rules are introduced for very large online platforms and very large online search engines that reach more than 45 million users, given their systemic impact in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas. When such platforms recommend content, users can modify the criteria used, and choose not to receive personalised recommendations. Citizens don't have to take these companies at their word and can now scrutinise their actions through the reports of independent auditors and vetted researchers.
- **Clearer consequences**: Users can seek compensation from providers of intermediary services for any damage or loss suffered due to an infringement of the DSA by such provider.

What measures does the legislation take to counter illegal content?

The Digital Services Act sets out effective means for all actors in the online ecosystem to counter illegal content, but also illegal goods and services:

- Users are empowered to report illegal content in an easy and effective way.
- A priority channel will be created for trusted flaggers – entities which have demonstrated particular expertise and competence – to report illegal content to which platforms will have to react with priority. Trusted flaggers will be appointed from 17 February 2024 by Digital Services Coordinators, the national authorities in charge of supervising and enforcing the DSA in Member States.
- The DSA ensures that orders to act against illegal content, which are issued by the relevant national judicial or administrative authorities on the basis of the applicable Union law or national law in compliance with Union law, can be complied with in an effective and efficient manner, in particular in a cross-border context. Very large online platforms will need to take mitigating measures at the level of the overall organisation of their service to protect their users from illegal content, goods and services.

How does the DSA protect people from unsafe or counterfeit goods?

The Digital Services Act sets out effective means for all actors in the online ecosystem to counter illegal goods:

- Platforms have mandatory procedures in place for removing illegal goods.
- Online marketplaces are also requested to trace their traders ("know your business customer"). This ensures a safe, transparent and trustworthy environment for consumers and discourage traders who abuse platforms from selling unsafe or counterfeit goods.
- Online platforms are requested to organise their online interfaces in a way that allows traders to comply with their information obligations towards consumers.
- A new system of trusted flaggers will also be available from 17 February 2024[PP(1)] [O(2)] [O(3)] [Z(4)] , for example, for brand owners fighting counterfeit goods, and for faster and easier flagging and removal of counterfeit goods.
- Public authorities have new tools to order the removal of unsafe products directly.
- Marketplaces are also required to implement reasonable efforts to randomly check whether products or services have been identified as being illegal in any official database and take the appropriate action.
- Very large online platforms are subject to an audited risk assessment that includes an analysis on their vulnerability to illegal goods on their platforms, and their mitigation measures at this organisational level are now also subject to annual audits.

How does the DSA protect minors?

Under the DSA, providers of online platforms that are accessible to minors are required to put in place appropriate measures to ensure high level of privacy, safety and security of minors on their services.

In addition, the new rules ban targeted advertising to minors based on profiling using the personal data of users of their services when they can establish with reasonable certainty that the recipient of the service is a minor.

How can harmful but not illegal content be effectively addressed?

To the extent that it is not illegal, harmful content should not be treated in the same way as illegal content. The new rules only impose measures to remove or encourage removal of illegal content, in full respect of the freedom of expression.

At the same time, the DSA regulates very large online platforms and very large online search engines responsibilities when it comes to systemic issues such as disinformation, hoaxes and manipulation during pandemics, harms to vulnerable groups and other emerging societal harms. Following their designation by the Commission, very large online platforms and very large online search engines that reach at least 45 million users have to perform an annual risk assessment and take corresponding risk mitigation measures stemming from the design and use of their service. Any such measures need to be carefully balanced against restrictions of freedom of expression. They also need to undergo an independent audit.

In addition, the proposal sets out a co-regulatory framework where service providers can work under codes of conduct to address negative impacts regarding the viral spread of illegal content as well as manipulative and abusive activities, which are particularly harmful for vulnerable recipients of the service, such as children and minors.

The DSA fosters a co-regulatory framework for online harms, including codes of conduct, such as a revised Code of Practice on disinformation, and crisis protocols.

How will you keep a fair balance with fundamental rights such as the freedom of expression?

The DSA protects freedom of expression, including freedom and pluralism of the media. It does so by striking a delicate balance between creating rules to tackle illegal content and safeguarding freedom of expression and information online. This includes protection from government interference in people's freedom of expression and information. The horizontal rules against illegal content are carefully calibrated and accompanied by robust safeguards for freedom of expression and an effective right of redress – to avoid both under-removal and over-removal of content on grounds of illegality.

Here are three examples of how freedom of expression is protected by the DSA:

1. **Complaint mechanism to appeal moderation decisions**: The DSA gives users the possibility

to contest the decisions taken by the online platforms to remove their content, including when these decisions are based on platforms' terms and conditions. If an account or a piece of content is suspended or otherwise limited, users have the right to contest the decision. This ensures that decisions are not arbitrary and empowers users to protect their online presence. Users can complain directly to the platform, choose an out-of-court dispute settlement body or seek redress before Courts.

2. **The DSA requires platforms to be transparent in their content moderation**: The Digital Services Act sets rules on transparency of content moderation decisions. For example, the DSA mandates transparency around 'shadow banning' and similar content moderation. When an account gets restricted, the user must be informed and has the right to appeal the decision. Service providers are also required to disclose their moderation policies and how they are implemented, building trust and clear communication between platforms and users. For very large platforms, users and consumers can have a better understanding of the ways these platforms impact our societies. Very large platforms are obliged to mitigate those risks, including as regards freedom of expression. They will be held accountable through independent auditing reports and specialised and public scrutiny.
3. **Addressing biases in recommender algorithms:** The DSA introduces new tools to assess and rectify biases in recommender systems. These provisions are aimed at creating a more fair and representative online experience, respecting the diversity and individuality of users.

All the obligations in the DSA, including the crisis response mechanism, are carefully calibrated to promote the respect of fundamental rights, such as freedom of expression.

How does the Digital Services Act tackle disinformation?

Through its rules on how platforms moderate content, on advertising, algorithmic processes and risk mitigation, the DSA aims to ensure that platforms – and in particular the very large ones – are more accountable and assume their responsibility for the actions they take and the systemic risks they pose, including on disinformation and manipulation of electoral processes.

The Digital Services Act fosters a co-regulatory framework, together with the updated Code of Practice on Disinformation and the new Commission Guidance, as announced in the European Democracy Action Plan.

How does the Digital Services Act regulate online advertising?

The Digital Services Act covers any type of advertising, from digital marketing to issues-based advertising and political ads, and complements existing rules such as the General Data Protection Regulation, which already establishes, for example, rules on users' consent or their right to object to targeted digital marketing.

The DSA introduces two new restrictions concerning targeted advertising on online platforms. First, it bans targeted advertising of minors based on profiling. Second, it bans targeted advertising based on profiling using special categories of personal data, such as sexual orientation or religious beliefs.

The new rules empower users in understanding and making informed decisions about the ads they see. They have to be clearly informed whether and why they are targeted by each ad and who paid for the ad; they should also see very clearly when content is sponsored or organically posted on a platform and should also see when influencers are promoting commercial messages. Notice and action obligations also apply for potentially illegal ads, as for any other type of content.

For very large online platforms, the societal stakes are higher, and the rules include additional measures to mitigate risks and enable oversight. They have to maintain and provide access to ad repositories, allowing researchers, civil society and authorities to inspect how ads were displayed and how they were targeted. They also need to assess whether and how their advertising systems are manipulated or otherwise contribute to societal risks, and take measures to mitigate these risks.

The rules are complemented by measures in the Digital Markets Act, which tackles the economic concerns over gatekeepers' advertising models.

How does the Digital Services Act protect personal data?

The DSA has been designed in full compliance with existing rules on data protection, including the General Data Protection Regulation (GDPR) and the ePrivacy Directive, and does not modify the rules and safeguards set out in these laws.

How does the Digital Services Act address dark patterns?

Under the DSA, dark patterns are prohibited. Providers of online platforms are now required not to

design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of users of their services to make free and informed decisions.

The ban complements, but does not overwrite the prohibitions already established under consumer protection and data protection rules, where large numbers of dark patterns that mislead consumers are already banned in the EU.

3. Impact on businesses

What digital services does the act cover?

The Digital Services Act applies to a wide range of online intermediaries, which include services such as internet service providers, cloud services, messaging, marketplaces, or social networks. Specific due diligence obligations apply to hosting services, and in particular to online platforms, such as social networks, content-sharing platforms, app stores, online marketplaces, and online travel and accommodation platforms. The most far-reaching rules in the Digital Services Act focus on very large online platforms and very large online search engines, which have a significant societal and economic impact, reaching at least 45 million users in the EU (representing 10% of the population). Very large online platforms and very large online search engines are designated by the Commission and, after their designations, have 4 months to comply with the additional obligations applicable specifically to very large online platforms/search engines, such as the risk management obligations, obligations to provide access to data for vetted researchers and obligations to submit their services to an audit.

What impact will the Digital Services Act have on businesses?

The DSA modernises and clarifies rules dating back to the year 2000. It sets a global benchmark, under which online businesses benefit from a modern, clear and transparent framework assuring that rights are respected and obligations are enforced.

Moreover, for online intermediaries, and in particular for hosting services and online platforms, the rules cut the costs of complying with 27 different regimes in the single market. This is particularly important for innovative SMEs, start-ups and scale-ups, in order to scale at home and compete with very large players. Small and micro-enterprises are exempted from some of the rules that might be more burdensome for them. The Commission is carefully monitoring the effects of the new Regulation on SMEs.

Other businesses also benefit from the new set of rules. With the DSA, they have access to simple and effective tools for flagging illegal activities that damage their trade, as well as internal and external redress mechanisms, affording them better protections against erroneous removal, limiting losses for legitimate businesses and entrepreneurs.

Furthermore, those providers which voluntarily take measures to further curb the dissemination of illegal content are reassured that these measures cannot have the negative consequences of being unprotected from legal liability.

How does the Digital Services Act support start-ups and innovation in general?

With a single framework for the EU, the DSA makes the single market easier to navigate, lowering compliance costs and establishing a level playing field. Fragmentation of the single market disproportionately disadvantages SMEs and start-ups wishing to grow, due to the absence of a large enough domestic market and to the costs of complying with many different legislations. The costs of fragmentation are much easier to bear for businesses, which are already large.

A common, horizontal, harmonised rulebook applicable throughout the Digital Single Market gives SMEs, smaller platforms and start-ups, access to cross-border customers in their critical growth phase. The rules are accompanied by standardisation actions and Codes of Conduct that should support a smooth implementation by smaller companies.

How does the Digital Services Act differentiate between small and big players?

The DSA sets asymmetric due diligence obligations on different types of intermediaries depending on the nature of their services as well as on their size and impact, to ensure that their services are not misused for illegal activities and that providers operate responsibly. Certain substantive obligations are limited only to very large online platforms, which have a central role in facilitating the public debate and economic transactions. Very small platforms are exempt from the majority of obligations.

By rebalancing responsibilities in the online ecosystem according to the size of the players, the DSA ensures that the regulatory costs of these new rules are proportionate.

What impacts does the proposed Digital Services Act have on platforms and very large

platforms?

All platforms, except the smallest (employing fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed €10 million), are required to set up complaint and redress mechanisms and out-of-court dispute settlement mechanisms, cooperate with trusted flaggers, take measures against abusive notices, deal with complaints, vet the credentials of third party suppliers, and provide user-facing transparency of online advertising.

In addition, very large online platforms and very large online search engines, reaching at least 45 million users (i.e. representing 10% of the European population) are subject to specific rules due to the particular risks they pose in the dissemination of illegal content and societal harms.

Very large online platforms have to meet risk management obligations, external risk auditing and public accountability, provide transparency of their recommender systems and user choice for access to information, as well as share data with authorities and researchers.

4. Impact on Member States

How can the gaps between laws in Member States be filled?

The experience and attempts of the last few years have shown that individual national action to rein in the problems related to the spread of illegal content online, in particular when very large online platforms are involved, falls short of effectively addressing the challenges at hand and protecting all Europeans from online harm. Moreover, uncoordinated national action puts additional hurdles on the smaller online businesses and start-ups who face significant compliance costs to be able to comply with all the different legislation. Updated and harmonised rules better protect and empower all Europeans, both individuals and businesses.

The Digital Services Act provides one set of rules for the entire EU. All citizens in the EU have the same rights, a common enforcement system sees them protected in the same way and the rules for online platforms are the same across the entire Union. This means standardised procedures for notifying illegal content, the same access to complaints and redress mechanisms across the single market, the same standard of transparency of content moderation or advertising systems, and the same supervised risk mitigation strategy where very large online platforms are concerned.

At the same time, as a Regulation, the Digital Services Act applies directly superseding overlapping national laws that follow the same objective. Besides, as the DSA is a full harmonisation instrument, EU Member States cannot go beyond the Regulation in their national laws.

Which institutions supervise the rules, and who selects them?

The supervision of the rules is shared between the Commission – primarily responsible for platforms and search engines with more than 45 million users in the EU – and Member States, responsible for any smaller platforms and search engines according to the Member State of establishment.

The Commission has the same supervisory powers as it has under current anti-trust rules, including investigatory powers and the ability to impose fines of up to 6% of global revenue.

Member States are required to designate competent authorities – referred to as Digital Services Coordinators – by 17 February 2024, to supervise compliance of the services established on their territory with the new rules, and to participate in the EU cooperation mechanism of the proposed Digital Services Act. The Digital Services Coordinator is an independent authority with strong requirements to perform their tasks impartially and with transparency. The new Digital Services Coordinator within each Member State will be an important regulatory hub, ensuring coherence and digital competence.

The Digital Services Coordinators will cooperate within an independent advisory group, called the European Board for Digital Services, which can support with analysis, reports and recommendations, as well as coordinating the new tool of joint investigations by Digital Services Coordinators.

The European Board for Digital Services will be established on 17 February 2024.

What is the Commission's role in the supervision of platforms?

The enforcement of the Digital Services Act for providers of intermediary services established on their territory is primarily a task for national competent authorities, notably the Digital Services Coordinators.

However, when it comes to supervision of very large online platforms and online search engines, the Commission is the sole authority to supervise and enforce the specific obligations under the DSA that apply only to these providers. In addition, the Commission will be, together with the Digital Services

Coordinators, also responsible for supervision and enforcement for any other systemic issue concerning very large online platforms and very large online search engines.

An important part of the supervisory and enforcement framework under the DSA will also be the Board, whose members will be independent Digital Services Coordinators.

What penalties do businesses face if they do not comply with the new rules?

The new enforcement mechanism, consisting of national and EU-level cooperation, will supervise how online intermediaries adapt their systems to the new requirements. Each Member State will need to appoint a Digital Services Coordinator, an independent authority responsible for supervising the intermediary services established in their Member State and/or for coordinating with specialist sectoral authorities. To do so, it will impose penalties, including financial fines. Each Member State must clearly specify the penalties in their national laws in line with the requirements set out in the Regulation, ensuring they are proportionate to the nature and gravity of the infringement, yet dissuasive to ensure compliance.

For the case of very large online platforms and very large online search engines, the Commission has direct supervision and enforcement powers and can, in the most serious cases, impose fines of up to 6% of the global turnover of a service provider.

The enforcement mechanism is not only limited to fines: the Digital Services Coordinator and the Commission will have the power to require immediate actions where necessary to address very serious harms, and platforms may offer commitments on how they will remedy them.

For rogue platforms refusing to comply with important obligations and thereby endangering people's life and safety, it will be possible as a last resort to ask a court for a temporary suspension of their service, after involving all relevant parties.

Does the DSA already apply?

The rules apply in two steps:

The DSA is directly applicable across the EU from 17 February 2024. By 17 February, Member States have to appoint national authorities to enforce the rules on smaller platforms and rules concerning non-systemic issues on very large online platforms and very large online search engines.

For very large online platforms and very large online search engines, which are directly supervised by the Commission as regards systemic obligations, the new rules kicked in earlier. First and foremost, all online platforms, except micro and small ones, were required to publish information on the number of active monthly users by 17 February 2023, an exercise which must be repeated at least once every 6 months afterwards. They are also invited to communicate these numbers to the Commission, which is responsible for assessing whether they reach threshold of 45 million users and should therefore be designated as very large online platforms or very large online search engines.

Once designated by the Commission, providers of very large platforms and very large online search engines have four months to comply with the DSA, including to undertake and provide to the Commission first risk assessment under the DSA. Therefore, for the first set of designated very large platforms and very large online search engines, the additional obligations started to apply at the end of August 2023. For the second set of designated very large online platforms and very large online search engines, the additional obligations start to apply from the end of April 2024.

More information is available here.

5. European Centre for Algorithmic Transparency

What technical expertise does the Commission have to supervise the biggest online intermediaries?

Since the end of the negotiations, the Commission has been preparing to take on the responsibility of supervising very large online platforms and search engines under the DSA, including efforts to increase staffing and expertise in the field of data science and algorithms, amongst others.

The Commission's supervisory role is enhanced by the European Centre for Algorithmic Transparency, housed in the Commission's Joint Research Centre (JRC). The Centre contributes with technical expertise, scientific research and foresight to the Commission's exclusive supervisory and enforcement role of the systemic obligations on very large online platforms and search engines provided for under the DSA. It counts on a team of specialised experts, who also work on identifying and measuring systemic risks.

The ECAT was formally launched in April 2023. While most of its staff is located in the Joint Research

Centre site based in Seville, Spain, it also works closely with JRC colleagues based in Ispra, Italy and Brussels, Belgium.

What is the role of the European Centre for Algorithmic Transparency?

The Centre provides in-house technical assistance in the area of algorithmic systems linked to the DSA's aim of ensuring a safe, predictable and trusted online environment, drawing from expertise in different disciplines to integrate technical, ethical, economic, legal and environmental perspectives.

The Centre centralises research with a focus on algorithmic transparency, ensuring that decisions made by algorithms supporting the provision of digital services are transparent, explainable and in line with the risk management obligations of the very large online platforms and search engines.

6. The enforcement framework

What type of investigatory powers does the Commission have?

The Commission is the sole authority to supervise and enforce the specific obligations under the DSA that apply only to very large online platforms and very large online search engines. To monitor their compliance with the DSA, the Commission has investigative and enforcement powers, which are inspired by similar powers existing under competition rules.

To gather information, in the case of a suspicion of infringement of the DSA, the Commission can, inter alia:

- Send a request for information (RFI) to verify platforms' compliance with the DSA. The Commission can send simple RFIs, or RFIs by decision. RFIs sent by decision legally oblige providers to reply.
- Order access to the very large online platform' or very large online search engine's data and algorithms, e.g. to assess how the algorithm/recommender system of a platform promotes illegal content.
- Conduct interviews of any person who might have information on the subject matter of an investigation.
- Conduct inspections at the very large online platforms' premises with the support of the DSC of the Member State of establishment, when relevant, who may need to request an authorisation issued by a judge.

More information is available here.

What can the Commission do if it has suspicions that a very large online platform or a very large online search engine does not comply with the DSA?

If the Commission suspects that a very large online platform or a very large online search engine has infringed any of the DSA's provisions, the Commission can adopt a decision to open a **formal proceeding**. The opening of a proceeding is a legal requirement for taking further enforcement steps.

After the opening of a proceeding, the Commission can continue to gather information about the investigated conduct, for example by sending a request for information, conducting interviews, or doing inspections.

The Commission can at any time conclude the entire or parts of the proceedings, for example if the in-depth investigation does not allow to confirm a suspected infringement mentioned in the opening decision.

Should the Commission conclude during a formal proceeding that there is an infringement of the DSA, it can take further enforcement steps, which may include:

- **Interim measures**: where there is an urgency due to the risk of serious damage for users, the Commission can require immediate actions to address such harms. Any measure taken should be proportionate and temporary to mitigate such a risk. Examples of interim measures can be changes to recommender systems, increased monitoring of specific keywords or hashtags, or orders to terminate or remedy alleged infringements.
- **Binding commitments**: concerned providers can make commitments to the Commission to ensure compliance with the DSA. Should the Commission consider them effective, it can accept these commitments by adopting a decision.
- **Non-compliance decision**: if the Commission finds that the DSA, the ordered interim measures, or the made commitments have been breached, it can adopt a non-compliance decision.

Following a non-compliance decision, the Commission can impose fines up to 6% of the global turnover of the provider concerned and order that provider to take measures to address the breach by the deadline set by the Commission. That decision may also trigger an enhanced supervision period to ensure compliance with the measures the provider intends to take to remedy the breach. In the case of a non-compliance decision due to a procedural breach (e.g. supply of incorrect, misleading or incomplete information to a request for information), the Commission can impose fines up to 1% of annual worldwide turnover. The Commission can also impose periodic penalty payment to incentivise a platform to comply.

The DSA does not set any legal deadline for bringing formal proceedings to an end. The duration of an in-depth investigation depends on a number of factors, including the complexity of the case, the extent to which the company concerned cooperate with the Commission and the exercise of the rights of defence.

What type of sanctioning powers does the Commission have?

The Commission can **apply fines up to 6%** of the worldwide annual turnover in case of breach of the DSA following a non-compliance decision, or failure to comply with interim measures, or breach of commitments. The Commission can also apply **periodic penalties up to 5%** of the average daily worldwide turnover for each day of delay in complying with remedies, interim measures, commitments.

As a last resort measures, if the infringement persists and causes serious harm to users and entails criminal offences involving threat to persons' life or safety, the Commission can request the Digital Services Coordinator of the Member State concerned to request national courts to temporarily restrict access of recipients to the service, following a specific procedure.

The Commission can use its enforcement powers in justified cases of ensuring compliance with the DSA and to the extent this is necessary and proportionate. All Commission decisions are subject to judicial redress before the Court of Justice of the EU.

How does the Commission finance costs associated with the new supervisory and enforcement competences?

In order to ensure effective compliance with the DSA, it is important that the Commission has at its disposal necessary resources, in terms of staffing, expertise, and financial means, for the performance of its tasks under this Regulation. To this end, starting from the end of 2023, the Commission charges supervisory fees on providers of very large online platforms and search engines, the level of which is established on an annual basis. The overall amount of annual supervisory fees charged is established on the basis of the overall amount of the costs incurred by the Commission to exercise its supervisory tasks under this Regulation, as reasonably estimated beforehand.

The annual supervisory fee charged to providers of very large online platforms and search engines is proportionate to the size of the service as reflected by the number of its recipients in the Union. To this end, as long as the conditions established in the provisions of the Delegated Regulation are met, the individual annual supervisory fee does not exceed an overall ceiling (set at 0.05% of the annual worldwide net income) for each provider of very large online platforms and very large online search engines, in order to take into account the economic capacity of the provider of the designated service or services.

Detailed rules specifying the procedure and detailed methodology for the application of the supervisory fees were adopted by the Commission on 2 March 2023, and sent to the European Parliament and Council for their three months scrutiny, before publication and entry into force. In accordance with the procedure envisaged in the Delegated Regulation, the Commission prepared an estimation of costs which are divided amongst the services that are designated as very large online platforms or very large online search engines before 31 August 2023. Each individual fee depends on a number of factors as described in the act, including the number of active recipients that they have. The decisions setting the individual amounts of the fees to be charged were taken in November 2023, and these amounts are to be paid at the latest by 31 December 2023.

**Updated on 23/02/2024*

QANDA/20/2348

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Thomas Regnier (+32 2 29 9 1099)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email