Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

DIGITAL SERVICES ACT
PART II: DUE DILIGENCE OBLIGATIONS

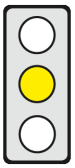
cep**PolicyBrief** No. 23/2021

KEY ISSUES

Background: Digital services acting as intermediaries, i.e., connecting users with suppliers of goods, services and content, are increasingly being misused to spread illegal content online. The providers of such services thus play a central role in combating illegal content but lack transparency on how they moderate – e.g., remove – content.

Objective of the Regulation: The Commission wants to regulate and harmonise the responsibilities and accountability of providers of intermediary services, including online platforms, and the oversight and enforcement procedures, in order to improve the internal market for such services and create a safe and transparent online environment.

Affected parties: Providers of intermediary services, including online platforms, e.g. social media and marketplaces, business and private users ("recipients") of intermediary services.



Pro: (1) The introduction of a notice and action mechanism will facilitate the removal of illegal content.

(2) Scaled obligations are important in order to ensure proportionality.

Contra: (1) Obligations for very large online platforms (VLOPs) should also apply to smaller platforms if these platforms pose certain "systemic" risks yet to be defined in more detail.

(2) Empowering the Commission to specify who is an "active user" of a platform and how to determine their number of recipients, is in breach of EU law. These fundamental questions must be regulated directly by the DSA.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM(2020) 825 of 15 December 2020 for a **Regulation** of the European Parliament and of the Council **on a Single Market for Digital Services (Digital Services Act)** and amending Directive 2000/31/EC

Brief Summary

- **Objectives and Definitions**
  - Digital services acting as intermediaries, i.e., connecting users with suppliers offering goods, services and content, are increasingly being misused to spread illegal content online. The providers of such services thus play a central role in combating illegal content but lack transparency on how they moderate – e.g., remove – content.
  - With the Digital Services Act (DSA), the Commission wants to update and harmonise the responsibilities and accountability of providers of intermediary services (ISPs) in order to
    - improve the internal market for intermediary services (IS) and
    - create a safe and transparent online environment where fundamental rights are protected, e.g. freedom of expression, freedom of information and freedom to conduct a business [Art. 1].
  - IS are access, caching or hosting services [Art. 2 (f), (b), see cep**PolicyBrief** No. 22/2021].
  - Hosting services consist of storing content provided by the users ("recipients") of the service at their request, e.g. video streaming and cloud services and online platforms such as marketplaces and social media.
  - Illegal content is any information which [Art. 2 (g), Recital 12]
    - under national or EU law, is either illegal per se – e.g. terrorist content –, or
    - relates to illegal activities, products or services, e.g. the sale of counterfeit products.
  - The DSA sets out harmonised
    - liability exemptions for ISPs [see cep**PolicyBrief** No. 22/2021],
    - due diligence obligations for ISPs, tailored to specific categories of ISPs [this cep**PolicyBrief**],
    - rules on oversight, cooperation and enforcement [cep**PolicyBrief** No. 24/2001].

- **Due Diligence Obligations for all ISPs**
  - The Commission wants to establish clear and balanced due diligence obligations for ISPs [Recital 34]. ISPs must
    - designate a liable legal representative if they are not based in the EU [Art. 2 (d), Art. 11];
    - establish a single contact point for communication, inter alia with authorities and the Commission, and specify one or more official EU languages for communication, including at least one of the official languages of the country in which the ISP or its legal representative is established [Art. 10];
    - explain in their terms and conditions ("T&Cs") how they restrict and moderate – e.g., remove – content that is illegal or incompatible with their T&Cs, e.g., by using algorithms, and must respect the fundamental rights of the recipients of their service and rights of other parties when restricting content [Art. 2 (p), 12]; and

Authors: Anja Hoffmann, Matthias Kullas, Andrea DePetris and Victor Warhem | kullas@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone + 49 761 38693-0 | www.cep.eu

- outline their content moderation activities in annual transparency reports (Art. 13), except small ISPs.

- **Additional Due Diligence Obligations for Providers of Hosting Services, including Online Platforms**
  - Furthermore, providers of hosting services must
    - establish user friendly electronic "notice and action mechanisms" allowing users to notify illegal content on their services [Art. 14]; all notices must contain the exact URL of the content and a reasoning why it is illegal;
    - inform the recipients affected by their decision to remove or block content, and provide a statement of reasons which must contain further details, inter alia on the use of automated means in taking the decision [Art. 15].
  - If a provider of hosting services receives a notice that a specific item of content is illegal, it will be considered to have knowledge or awareness of the illegality. The provider will not be able to invoke the liability exemptions unless it acts expeditiously to remove or block this content. [Art. 14 (3), Art. 5 (1), see cep**PolicyBrief** No. 22/2021]

- **Additional Due Diligence Obligations for Online Platforms**
  - Online platforms are providers of hosting services that not only store third party content but also – at their recipients' request – disseminate that content to the public, e.g. social networks, marketplaces and travel platforms, unless such dissemination is purely ancillary to their principal service [Art. 2 (h), Recital 13].
  - Online platforms – except small ones [Art. 16] – must fulfil additional due diligence obligations. They must, e.g.,
    - decide with priority upon notices submitted by "trusted flaggers" – independent entities may be granted such status if they meet harmonized conditions, e.g., represent collective interests and have expertise [Art. 19];
    - enable their recipients to resolve disputes about a platform's decision to remove content or to suspend its services via an internal complaint handling system [Art. 17], and through the binding decision of a certified independent out-of-court dispute settlement body which has expertise and follows fair rules [Art. 18];
    - take action against misuse, e.g. temporarily suspend their services to "frequent" providers of "manifestly" illegal content, or cease handling complaints from individuals who "frequently" file "manifestly" unfounded complaints [Art. 20];
    - notify suspicions of serious criminal offences to the competent law enforcement or judicial authorities [Art. 21];
    - ensure that users are able to identify advertisements as such, to see on whose behalf they are displayed and to identify the main parameters used to determine why an advertisement is shown to them [Art. 24];
    - trace traders and make the advertising, offering and distance selling of products or services to consumers via their platforms conditional upon the provision of reliable information on traders, e.g. contact and bank details and a self-certification that it only offers lawful products or services ["know your business customer", Art. 22].

- **Additional Due Diligence Obligations for Very Large Online Platforms (VLOPs)**
  - Very large online platforms (VLOPs) are platforms which have at least 45 million "average monthly active recipients" in the EU – i.e. 10% of its population – and which have been designated as a VLOP by the Digital Services Coordinator, an authority designated by the Member State in which the platform is established [Art. 25].
  - The Commission will adopt delegated acts on how to calculate or adjust the number of recipients [Art. 25 (3)].
  - The Commission wants to impose additional due diligence obligations on VLOPs. Due to their reach, VLOPs play a central role in facilitating public debates and economic transactions, and in influencing how recipients obtain and communicate information; thus, they pose higher societal risks. [Recital 53]
  - VLOPs must regularly assess significant systemic risks stemming from the use or misuse of their service [Art. 26]:
    - the dissemination of illegal content, e.g. through accounts with a wide reach;
    - negative effects, e.g. of algorithms, on fundamental rights like the freedom of expression;
    - intentional manipulation of their services with an impact e.g. on public health, civic discourse, public security and electoral processes, e.g. through the use of fake accounts or bots.
  - When assessing systemic risks, VLOPs must also analyse their automated systems [Art. 2 (n)-(p), Art. 26 (2)]:
    - content moderation systems aimed at detecting and restricting illegal content,
    - recommender systems that suggest information to recipients or determine the order in which it is shown, and
    - advertising systems, which display advertisements that promote messages of any kind in return for payment.
  - VLOPs must adopt adequate measures to mitigate these risks, e.g. adapt their content moderation or recommender systems, or cut advertising revenue for certain content [Art. 27, Recital 58].
  - In addition, VLOPs must, inter alia,
    - publicly archive displayed advertisements and related data, e.g. parameters for targeted advertising [Art. 30];
    - undergo yearly independent audits to verify their compliance with all due diligence obligations and voluntary commitments and, in case of a negative audit report, implement the recommended measures [Art. 28];
    - disclose the main parameters used in their recommender systems to prioritise information as well as the options for modifying them; the recipients must be able to choose an option that is not based on profiling – i.e. on the creation of a personal profile through an automated analysis of collected personal data [Art. 29];
    - provide supervisory authorities and researchers with access to its data for monitoring purposes [Art. 31]; and
    - appoint a qualified compliance officer as its advisor and supervisor for compliance [Art. 32].

Statement on Subsidiarity by the Commission

The conditions for cross-border digital services can only be harmonised at EU level (see cep**PolicyBrief** No. 22/2021).

Policy Context

The DSA builds on consultations carried out by the Commission. The European Parliament has released resolutions [2020/18/INL, 2020/19/INL and 2020/2022/INI] with recommendations. Together with the Digital Markets Act (see cep**Input** No. 12/2021, cep**PolicyBriefs** No. 14/2021 and 15/2021), the DSA forms part of the Commission's proposal on new rules for digital platforms.

Legislative Procedure

15.12.20	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorates General:	DG Communications Networks, Content and Technology
Committees of the European Parliament:	IMCO (leading), Rapporteur: Christel Schaldemose (Denmark, S&D), LIBE, JURI, ITRE, ECON TRAN, CULT, FEMM
Federal Germany Ministries:	Economic Affairs (leading)
Committees of the German Bundestag:	Open
Decision-making Mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Competence:	Art. 114 TFEU (Internal Market)
Type of Legislative Competence:	Shared competence [Art. 4 (2) TFEU]
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

A single point of contact will facilitate the service and enforcement of judicial or administrative orders. This is why it is also necessary for ISPs, without an establishment in the EU, to designate a legal representative. In order to enable effective cross-border enforcement of the DSA, ISPs should be obliged to communicate with authorities and courts in English, where requested, in addition to an official language of their own choosing.

The introduction of a notice and action mechanism will facilitate the removal of illegal content. The DSA should also, however, regulate the language used for notices and e.g. stipulate that users can at least submit notices in English. Indicating a URL is not always possible and may require too much effort where there is a large amount of illegal content on a website.

The fact that ISPs risk to lose the exemption from liability [cf. cep**PolicyBrief** No. 22/2021] as soon as they are informed of il-legal content by way of a notice, on the one hand, gives ISPs an incentive to quickly remove such content. On the other hand, there is a danger of over-blocking if ISPs act too hastily and also remove legal content due to a fear of liability.

An internal complaints-handling system will help to make it easier for platform providers to correct wrong decisions, thereby helping to protect the rights of those involved. However, the system should also be available where a platform decides not to remove content. Thus, platforms should also have to justify their decisions not to remove reported content.

The prioritised processing of notices from "trusted flaggers" will speed up the removal of illegal content. However, the fact that flaggers must represent collective interests unnecessarily reduces their number.

The duty to report suspicions of serious criminal offences should apply to all ISPs. The definition of a "serious" criminal offence must, however, be clarified.

The transparency obligations for advertising may protect against manipulation. In addition, a ban on personalised advertising aimed at minors should also be considered as the proposed improvements to make personalised advertising more recognisable are inadequate for this group.

Providers of live streaming services and search engines should be subject to certain DSA obligations, such as the additional obligations applicable to providers of hosting services.

Legal Assessment

Legislative Competence of the EU & Subsidiarity

The DSA is rightly based on the internal market competence [Art. 114 (1) TFEU] and, in the overall assessment, is compatible with the principle of subsidiarity [see cep**PolicyBrief** No. 22/2021].

Proportionality with Respect to Member States

The choice of a Regulation rather than a Directive is proportionate. In order to create a horizontal framework for the tackling of illegal content by ISPs that removes the existing legal differences, uniform and directly applicable rules are preferable. These will also facilitate the effective enforcement of obligations and Member States can still determine what constitutes illegal content and who is liable for it. The DSA is, however, disproportionate to the extent that its relationship to national law and the scope of its blocking effect are both unclear [see cep**PolicyBrief** No. 22/2021].

Compatibility with EU Law in Other Respects

The obligations applicable to ISPs interfere with their freedom to conduct a business [Art. 16 CFR]. However, they serve a legitimate purpose, namely the protection of conflicting fundamental rights, in particular the freedom of expression and information [Art. 11 CFR] on the one hand, and, on the other, users' rights to privacy [Art. 7, 8 CFR] as well as third-party intellectual property rights [Art. 17 CFR]. The stricter obligations upon VLOPs to identify and reduce "systemic risks" and to archive advertising are justified in principle as being for the protection of public security and health as well as democracy – recognised by the EU as objectives serving the general interest [Art. 2 TEU, CJEU C-402/05 P - Kadi and al Barakaat, para. 303 – Art. 52 Abs. 1 CFR]. Open public debate and the freedom to form an opinion are essential for fair democratic participation. The obligations for VLOPs are too vague, however. The DSA must be more specific about what the systemic risks are and when manipulations are likely to have a negative effect on society, e.g. on civic discourse.

Scaled obligations are important in order to ensure proportionality. However, scaling must firstly be made even more risk-based. Only ISPs whose activities pose a small risk of violating fundamental rights or the general interest should be exempt from the obligations for online platforms and VLOPs. Conversely, **obligations for VLOPs should also apply to smaller platforms** with fewer than 45 million users **if,** due to their risks in the individual case, **these platforms pose certain "systemic" risks – to be defined in more detail.** The "risk level" and thus the category of obligations applicable to an ISP should not be linked exclusively to its turnover, staff or user numbers. The existence of risks in the case of platforms with over 45 million users, and the non-existence of risks in the case of those with fewer than 5 million users, may however be presumed subject to rebuttal.

Empowering the Commission to specify, in delegated acts, **who is an "active user" of a platform and how to determine their user numbers, is in breach of EU law** [Art. 290 (1) TFEU]. **These fundamental questions must be regulated directly by the DSA.**

Secondly, the obligations for platforms must be tailored more specifically to the function(s) that a platform offers because illegality is often easier to identify in offers on marketplaces than in statements on social networks where complicated assessments regarding freedom of speech are required. Insofar as platforms function as marketplaces, they could thus be made subject to shorter deadlines for action than social networks.

The too-vague obligation to block individuals who "frequently" post "manifestly" illegal content or submit unfounded notices, violates the fundamental right to freedom of expression and information. The criteria for blocking users or those who submit notices must be regulated by the DSA and not left up to the platform.

Participation in out-of-court dispute resolution must also be voluntary for platforms; their right to judicial redress [Art. 47 CFR] means that they, like users, must also be entitled to have decisions of dispute resolution bodies reviewed by the courts.

The fact that ISPs must declare, in their terms and conditions, what content they remove beyond illegal content, and that, when removing it, they must take account of users' fundamental rights, increases transparency for all concerned and helps to ensure that ISPs do not remove content arbitrarily and also that they have regard for freedom of speech. The resulting interference with their freedom of contract is justified. Due to the high relevance of ISPs for public communications, the EU legislator has a fundamental legal obligation to also protect users' freedom of expression; the duties to ensure protection recognised by the CFR, ECHR and the CJEU [Case C-265/95 para. 32] are comparable in this respect. In order to create legal certainty, numerous clarifications are still necessary, e.g. in what language should users submit notices of illegal content and in what language should IPS provide their statement of reasons for their decisions e.g. to block content.

Impact on and Compatibility with German Law

Due to its primacy over national legislation, the DSA supersedes the provisions of the German Network Enforcement Act, [NetzDG] and the State Media Treaty [MStV] insofar as they impose parallel obligations on ISPs.

Summary of the Assessment

The introduction of a notice and action mechanism will facilitate the removal of illegal content. The prioritised processing of notices from "trusted flaggers" will speed up the removal of illegal content. However, the fact that flaggers must represent collective interests unnecessarily reduces their number. Scaled obligations are important in order to ensure proportionality. However, obligations for VLOPs should also apply to smaller platforms if these platforms pose certain "systemic" risks – to be defined in more detail. Empowering the Commission to specify who is an "active user" of a platform, and how to determine their user numbers, is in breach of EU law. These fundamental questions must be regulated directly by the DSA.