First report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risks as well as mitigation measures

18 November 2025

EUROPEAN BOARD FOR DIGITAL SERVICES

Table of content

1. What this report is about

The Digital Services Act ("DSA") regulates online intermediary services, platforms such as online marketplaces[1], social networks, application stores, or search engines. The supervision and enforcement of the rules in the DSA is carried out by the European Commission and by authorities in Member States, notably the national Digital Services Coordinators ("DSCs"), all of which work together in the European Board for Digital Services ("the Board").

The DSA risk management framework in Articles 34 and 35 establishes key obligations for providers of very large online platforms ("VLOPs") and of very large online search engines ("VLOSEs"). These services have at least 45 million monthly active recipients in the Union. Article 34(1) DSA establishes a requirement to *"diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services"*. Article 35(1) DSA requires that providers of VLOPs and VLOSEs take reasonable, proportionate and effective mitigation measures tailored to the systemic risks identified in their risk assessments. In doing so, providers must have particular consideration for the impacts of such measures on fundamental rights. Recital 90 of the DSA adds that providers of VLOPs and VLOSEs *"should ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights and that they test their assumptions with the groups most impacted by the risks and the measures they take"*. These provisions are applicable to VLOPs and VLOSEs, but not to platforms or other intermediary services under the threshold of 45 million average monthly active recipients in the Union.

1.1. Background to this report

Article 35(2) DSA sets out the requirement for the Board, in cooperation with the Commission, to publish comprehensive reports once a year. Article 35(2) DSA requires the identification and assessment of the most prominent and recurrent systemic risks in the Union and in the Member States, as well as best practices for their mitigation.

This first edition sets out the Board and the Commission's initial observations on systemic risks and related mitigation measures as they arise from the first experiences of designated VLOPs and VLOSEs with the implementation of the DSA. This report provides an overview of the most prominent and recurrent systemic risks that have been identified by the designated providers as stemming from their services as well as by stakeholders such as independent researchers and civil society organisations ("CSOs"), and an overview of certain risk mitigation practices. With regard to risk mitigation, this first edition focuses on practices that are in use or proposed. Over time, and based on accumulating experience with DSA implementation in

[1] Referred to as *"online platforms allowing consumers to conclude distance contracts with traders"* in the DSA.

practice, future editions of this report will also aim to identify evolving best practices in the mitigation of systemic risks.

1.2. The DSA risk management framework as a key safeguard for fundamental rights, including the right to freedom of expression and information

Ensuring that the rights enshrined in the Charter of Fundamental Rights of the European Union (the "Charter") are effectively protected online is one of the key objectives of the DSA, as is explicitly expressed in Article 1 on the aims of this Regulation. This first edition of the yearly reports pursuant to Article 35(2) DSA is therefore also an occasion to highlight that the risk management framework is a cornerstone of the DSA and, as such, it is a tool to support the protection of fundamental rights online.

Against this backdrop, the Board and the Commission recall that Article 34(1)(b) DSA requires VLOPs and VLOSEs providers to diligently identify, analyse and assess any actual or foreseeable negative effects for the exercise of fundamental rights.

During the preparation of this report, the Board and the Commission found that providers and CSOs observed systemic risks to the fundamental right to freedom of expression and information stemming from the design or functioning of the VLOP and VLOSE's services and their related systems or from the use made of their services.

- The Board and the Commission recall that Article 35(1) DSA requires VLOPs and VLOSEs providers to put in place reasonable, proportionate and effective mitigation measures, with particular consideration to the impact of such measures on fundamental rights including the right to freedom of expression and information enshrined in Article 11 of the Charter of Fundamental rights.

- The Board and the Commission also recall that recital 86 of the DSA states that: *"Providers of very large online platforms and of very large online search engines should deploy the necessary means to diligently mitigate the systemic risks identified in the risk assessments, in observance of fundamental rights.* (…) *Those providers should give particular consideration to the impact on freedom of expression".*

Beyond the risk management framework, the DSA also contains a comprehensive set of safeguards to protect the fundamental right to freedom of expression and information online in the Union:

- ***Complaint-handling mechanism for account suspensions:*** Article 20 DSA created a requirement for a timely, non-discriminatory, diligent and non-arbitrary internal complaint-handling mechanism for users. For example, if an account is suspended, its user has the right to contest that decision and receive a reply from the provider of the online platform.

- ***Transparency around content moderation:*** Article 17 DSA requires transparency around criteria for content moderation decisions, which includes "shadow banning" practices. For example, when an account is restricted, its user must be informed and has the right to contest that decision.

- ***Addressing biases in recommender systems:*** Articles 27 and 38 DSA introduced new tools to prevent or minimise biases in recommender systems by creating a requirement for providers of VLOPs and VLOSEs to allow users to be able to enjoy alternative options which are not based on profiling.

1.3. Reporting period and relationship with DSA enforcement activities

This report covers a reporting period between 17 February 2024 and 16 February 2025. This reporting period coincides with the start of application of the DSA's transparency reporting measures and lasts for one year from then on.

Nothing in this report should be interpreted as guidance for the compliance with Articles 34 or 35 DSA. Nothing in this report should be interpreted as constituting an assessment or evaluation of compliance by designated VLOPs and VLOSEs with Articles 34 or 35 DSA or any other provision of the DSA. This report is without prejudice to any current or future investigations, enforcement actions, or formal findings under the DSA.

2. How this report was prepared

This report was prepared on the basis of the following sources:

- The published versions of the risk assessment reports that providers of VLOPs and VLOSEs transmitted in 2023 and 2024 to the Commission and their DSC of establishment[2];
    - At the time of publication of this report, the first 17 VLOPs[3] and 2 VLOSEs[4] providers designated in April 2023 have carried out their first two yearly risk assessments in accordance with Article 34 DSA. Article 42 DSA further requires that these reports on risk assessments be submitted to the Commission and the DSC of their Member State of establishment and be made available to the public. For providers designated subsequently[5], the obligations under Article 34 also already apply and these providers have shared their first reports with the Commission and the DSC of their Member State of establishment as required by Article 42, but, as the obligation to make these first risk assessment reports available to the public was not yet applicable during this Article 35(2) report's reporting period, they are not covered in this Article 35(2) report. The Commission published a Q&A on risk assessment reports, audit reports and audit implementation reports under Article 42 DSA in November 2024 in order to provide more information about the reporting and publication obligations[6].
- The published versions of Article 37 DSA audit reports prepared by independent audit organisations;
    - At the time of publication of this report, the first 17 VLOPs and 2 VLOSEs providers designated in April 2023 have made the audit reports that they received from independent audit organisations available to the public.
- Other DSA transparency outputs prepared by VLOPs and VLOSEs providers:
    - Article 39 DSA advertisement repositories;
    - Article 37 DSA audit implementation reports, which are the reports that providers of VLOPs and VLOSEs must make available to the public one month after the receipt of the audit report from the independent audit organisation and in which they are to set out steps taken following recommendations of the audit organisation. At the time of publication of this report, the first 17 VLOPs and 2

[2] This European Commission webpage contains links to the webpages where providers published their DSA risk assessment reports: https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency#ecl-inpage-lsets8qr.
[3] Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter (now X), Wikipedia, YouTube, Zalando.
[4] Bing, Google Search.
[5] Pornhub, Shein, Stripchat, Temu, XNXX, XVideos.
[6] *"Q&A on risk assessment reports, audit reports and audit implementation reports under DSA"*, available at the following link: https://digital-strategy.ec.europa.eu/en/faqs/qa-risk-assessment-reports-audit-reports-and-audit-implementation-reports-under-dsa.

VLOSE providers designated in April 2023 have published audit implementation reports;

- Articles 15, 24 and 42(2) DSA transparency reports made available to the public by VLOPs and VLOSEs providers on content moderation;
- The DSA Transparency Database[7] that makes all Article 17 DSA statements of reasons available to the public. The DSA requires VLOPs and VLOSEs providers to inform their users of the content moderation decisions they take and explain the reasons behind those decisions in statements of reasons which they need to submit to the Transparency Database. The database enhances transparency and facilitate scrutiny over content moderation decisions as it allows to track the content moderation decisions taken by providers of online platforms in almost real-time.

- Input gathered through studies contracted by the Commission as well as by DSCs (these studies are mentioned in the Annex);
- Resources and studies from independent experts at research institutions and CSOs, including publications containing reactions to the risk assessment reports and other transparency outputs by providers of VLOPs and VLOSEs listed above, as well as input from CSOs, trusted flaggers[8] and Member State authorities collected by the Board and the Commission either upon invitation or through spontaneous submissions (these resources are listed in the Annex).
    - Amongst these sources, the Board and the Commission relied on the best available information and scientific insights currently available to determine which analyses and observations would contribute to the drafting of this report due to their relevance and quality. Future iterations of the yearly Article 35(2) DSA reports will benefit from further scientific insights based on data accessed via the mechanism of data access for researchers under Article 40 DSA. This report focuses on systemic risks and mitigation measures reported on by the VLOPs and VLOSEs providers. In addition, account was also taken of systemic risks and mitigation measures not mentioned by VLOPs and VLOSEs providers but that had been corroborated by several independent experts at research institutions and CSOs.

[7] DSA Transparency Database, available at the following link: https://transparency.dsa.ec.europa.eu/.
[8] According to Article 22 DSA, trusted flaggers are designated by Member States according to the following criteria: expertise and competence, independence, diligence, accuracy and objectivity.

3. The most prominent and recurrent systemic risks identified

This chapter follows the structure of Article 34(1) DSA in presenting an overview of the most prominent and recurrent systemic risks that may stem from VLOPs and VLOSEs. These systemic risks may materialise in different ways and to differing degrees on different services, depending amongst other things on the type of service and its use. For example, the most prominent and recurrent systemic risks on online marketplaces will be different from the most prominent risks on social media or mapping services. Generally, systemic risks related to illegal content or civic discourse are likely to manifest in different ways across Member States for example due to regional or linguistic aspects and different definitions of what constitutes illegal content in each Member State, while other systemic risks, such as those related to interface design, will generally likely be the same across the Union.

VLOPs and VLOSEs are evolving over time, and so do the ways users interact through them and with them, as well as the world in which they are used. There is a difference between a risk of harm and harm actually occurring. In the same vein, there is a difference between the risk of a violation of a right and an actual violation. The existence of a systemic risk means that the providers of VLOPs and VLOSEs must take measures to mitigate that risk (see Chapter 4 of this report on mitigation measures). This Chapter includes information on systemic risks. It does not present an overview of risks that would have materialised.

In addition to the systemic risks as such, this Chapter also presents examples of how certain risk factors mentioned in Article 34(2) influence those systemic risks. It is important to mention that these risk factors need to be considered both individually and in combination.

The mere fact that a systemic risk may be considered as recurrent does not mean that the risk remains unchanged. Also, as referred to in Article 35 DSA, specific developments in Member States may be relevant. All these changes affect how risks arise and evolve, and they make it necessary to constantly update relevant knowledge about systemic risks. In this regard, recital 90 of the DSA states that providers of VLOPs and VLOSEs:

- *"*[...] *should ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights and that they test their assumptions with the groups most impacted by the risks and the measures they take. To this end, they should, where appropriate, conduct their risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations. They should seek to embed such consultations into their methodologies for assessing the risks and designing mitigation measures, including, as appropriate, surveys, focus groups, round tables, and other consultation and design methods. In the assessment on whether a measure is reasonable, proportionate and effective, special consideration should be given to the right to freedom of expression".*

Furthermore, several provisions in the DSA enable a continuous examination of systemic risks. In addition to the risk assessments that providers of VLOPs and VLOSEs must carry out at least

once a year and prior to deploying functionalities that are likely to have a critical impact on the systemic risks identified, there are audit reports resulting from independent DSA compliance audits referred to in Article 37 DSA, audit implementation reports, transparency reports about content moderation practices on online platforms under Articles 15 and 42 DSA, as well as the rules on data access in Article 40 DSA.

The Sections below contain text boxes with examples of systemic risks. These are for illustration purposes only, in order to provide the reader with examples of how certain systemic risks have been presented by providers or CSOs. These text boxes do not constitute any evaluation of the approach of a provider. Furthermore, the choice and order of the quotes do not indicate that the risks they illustrate would be more important compared to other risks. Likewise, the text boxes in the Sections below on risk factors are there for illustration purposes only and do not constitute a comprehensive overview of the risk factors observed.

3.1. Illegal content

Contributing to combatting the dissemination of illegal content is a central objective of the DSA, as affirmed in several recitals, including recital 12, which emphasises the importance of *"a safe, predictable and trustworthy online environment"*. At the same time, the DSA is content-neutral and does not define what constitutes "illegal content". Instead, the legality of content is determined by Member State law other provisions of Union law. Article 3(h) DSA states that *"'illegal content' means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law"*. Article 34(1)(a) DSA requires that the risk assessments of designated VLOPs and VLOSEs include the systemic risks related to *"the dissemination of illegal content through their services"*.

Recital 80 of the DSA gives examples of illegal content that providers should assess: *"A first category concerns the risks associated with the dissemination of illegal content, such as the dissemination of child sexual abuse material or illegal hate speech or other types of misuse of their services for criminal offences, and the conduct of illegal activities, such as the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products, or illegally-traded animals"*.

The risk assessment and mitigation obligations of providers of VLOPs and VLOSEs in the DSA are part of a broader set of obligations. DSA provisions related to notice and action mechanisms (Article 16), trusted flaggers (Article 22) and orders to act against illegal content (Article 9) are central to the overall enforcement ecosystem concerning illegal content. Moreover, systemic risks linked to illegal content are addressed not only in the VLOPs and VLOSEs context, but also through other pieces of Union legislation, such as the Terrorist Content Regulation ("TCO")[9].

Actions carried out within the DSA to combat the dissemination of illegal content need to be aligned with fundamental rights, including the right to freedom of expression and information, which lie at the heart of the DSA. To this end, the DSA *inter alia* requires all online platforms to be transparent and enable scrutiny over their content moderation decisions, for example by requiring that providers inform users about their content moderation decisions and permit them to appeal those decisions. The DSA sets clear rules for transparency, accountability and user protection and empowerment.

Risks related to the dissemination of illegal content, including products, services and activities have been noted by all VLOPs and VLOSEs providers in their risk assessment reports. This Section outlines prominent and recurrent systemic risks identified in this context.

[9] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, available at the following link: https://eur-lex.europa.eu/eli/reg/2021/784/oj/eng.

This Section (and the rest of the report) uses in-line titles introduced at the beginning of certain paragraphs in bold and italics. These are intended to group systemic risks or mitigation measures into sub-categories for readability purposes.

Illegal products, services and activities. Systemic risks related to the dissemination of illegal products, services and activities, have been identified across all VLOPs and VLOSEs providers, in particular by online marketplaces (e.g. dangerous, non-compliant and/or counterfeit products), social media platforms (e.g. violent activities) and application stores (e.g. apps containing malware). Some providers presented systemic risks from products that may be compliant with the law but not with their terms and conditions together with systemic risks from illegal products, services and activities.

- ***The dissemination of illegal products***. Providers, in particular providers of online marketplaces, have reported systemic risks related to the sale and/or advertising of illegal products, such as products prohibited by Union or Member State law, including dangerous, non-compliant and/or counterfeit products (e.g. cosmetics, toys or electronic goods, firearms, explosives, hazardous chemicals). This has a negative impact notably on users which are exposed to illegal product listings, on the health and safety of consumers who buy such products, and on intellectual property ("IP") right holders. Some providers also noted that their services may be misused by traders using pseudonyms or fake company names. Similarly, CSOs noted the presence and availability of medical and healthcare products, such as prescription-only medicines, unauthorised psychoactive substances and counterfeit pharmaceuticals as a systemic risk.

- ***Illegal services and the conduct of illegal activities***. According to providers and CSOs, online platforms and search engines may be misused for a range of illegal services and activities. Amongst others, systemic risks identified include the provision or advertisement of illegal sexual services, such as prostitution (potentially linked to exploitation or trafficking), services enabling unauthorised entry, transit, or stay in the Union, and other services such as the recruitment into criminal networks, offers to abduct, hire to kill, or unlicenced offers of accommodation. Some providers also noted that their services may be misused for the sale or exchange of high amounts of cash currencies as well as illegal drugs, or to offer cyberattack services, including malware, phishing or inauthentic behaviour-for-hire (e.g. bots, fake identities), alongside identity theft and unauthorised access to user accounts. Other kinds of illegal content mentioned that are often closely tied to illegal services included the non-consensual sharing of intimate images or recordings, depictions of non-consensual sex, illegal pornography, and content linked to human trafficking or sexual exploitation. Violent or coercive content has also been reported as a systemic risk by VLOPs and VLOSEs providers and CSOs, such as content related to harassment, doxing, grooming, and threats to life.

Child Sexual Abuse Material ("CSAM"). Most VLOPs and VLOSEs providers and various CSOs have identified systemic risks related to the dissemination of CSAM, concerning in particular social media platforms and search engines. Specifically, providers reported risks that their users may be exposed to illegal content that sexualises minors, glorifies or facilitates child abuse, as well as grooming and sextortion. Section 3.4 gives further details on these systemic risks together with other systemic risks to the protection of minors.

Terrorist content. VLOPs and VLOSEs providers and CSOs have reported systemic risks related to terrorist content, concerning in particular social media platforms and search engines. These included risks of dissemination of terrorist imagery (in context other than for example journalistic purposes), praise, glorification, facilitation, support (such as fundraising), recruitment, radicalisation, and training of terrorists. Providers noted that the systemic risks extend to illegal content featuring for example symbols, flags, slogans, uniforms, gestures, salutes, or other elements representing violent extremist organisations or individuals. Under this category, some VLOPs and VLOSE providers as well as CSOs considered systemic risks related to content from sanctioned entities, for example from designated terrorist groups or sanctioned media organisations.

Illegal hate speech and the incitement of hate crimes. Providers, in particular of social media platforms and search engines, and CSOs identified different systemic risks related to the dissemination of illegal hate speech and the incitement of hate crimes. This report, and the DSA, rely on definitions of illegal hate speech from applicable Union and national laws, because the DSA itself does not define illegality. Within the Union legal framework, illegal hate speech primarily refers to speech targeting individuals or groups based on protected characteristics as set out in the Council Framework Decision 2008/913/JHA[10], namely race, colour, religion, descent, or national or ethnic origin. Some providers highlighted that this type of illegal content may lead to the dehumanisation, exclusion, segregation or vilification of individuals or groups, and may further lead to the promotion of violence against people that are categorised by others on the basis of specific characteristics. Providers are free to use additional elements in their own terms and conditions and policies in a way which may extend beyond the scope of illegal hate speech as defined by Union and Member States laws. For example, many providers have also defined as hate speech content which claims that individuals or groups with certain attributes/characteristics (i.e. age, sexual orientation and gender identity, or disability) are inferior or comparable to criminals, animals, or objects.

Intellectual property rights violations. Certain VLOPs and VLOSEs providers as well as CSOs have identified systemic risks related to content infringing IP rights, such as trademark, design rights, patent, and copyright, particularly in relation to counterfeit goods, pirated films and music, and illegal streaming services. These systemic risks concern in particular online marketplaces, social media services and search engines. Examples included the unauthorised

[10] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, available at the following link: https://eur-lex.europa.eu/eli/dec_framw/2008/913/oj/eng.

use of trademarks to create confusion, deception or misinterpretation regarding the source, origin, sponsorship, or affiliation of goods and services. The risk of IP rights violations was also recognised by certain providers as well as by the European Observatory on Infringements of Intellectual Property Rights of the EU Intellectual Property Office ("EUIPO") with regard to apps available on application stores, such as copycat apps or apps used to provide access to pirated content, particularly sports. Some VLOPs and VLOSEs providers also noted risks of copyright violations involving the sharing of musical works, audio files, audiovisual recordings, and other artistic works, including photographs, paintings, drawings, and other original visual renderings.

Consumer protection. Online marketplaces have reported various systemic risks related to consumer, some of which overlap with, *inter alia*, illegal content, such as the sale of non-compliant products or financial scams. Illegal content may directly impact consumer rights and safety. More information on systemic risks to consumer protection is available in Section 3.2 below.

Examples of risk factors concerning systemic risks related to illegal content:

Interface design and recommender systems: Providers and CSOs observed that the design of interfaces and recommender systems to stimulate engagement may result in the promotion of certain types of illegal content, as well as phenomena where users are repeatedly exposed to illegal content that aligns with their existing preferences.

Advertising systems: Providers and CSOs have mentioned similar risks with regard to advertising systems (e.g. due to targeted advertisement).

Content moderation systems: Across the board, techniques to evade detection such as coded language and links to off-platform interactions and transactions have been referenced by VLOPs and VLOSEs providers and CSOs. CSOs have also identified potential gaps in the moderation of certain languages, and stressed the importance of being able to understand local cultural references when moderating content. Risks related to manners to circumvent platform policies and content moderation measures through back-up content and profiles (i.e. duplicate pieces of content and accounts, which may even be referenced under the original restricted content and profiles) and outlinks to other platforms or websites have also been mentioned by CSOs. Audio, podcast and livestream content formats have been referred to as prone to circumventions of platforms policies and content moderation measures as content moderation systems may be less developed for audio formats.

Examples of observations concerning systemic risks related to illegal content:

Zalando, 2024 DSA risk assessment report, pp. 6-7: *"Zalando's online platform could be subject to the risk of spreading illegal content through either products themselves, products' presentation, advertising or communication content as well as customer reviews. These risks include, but are not limited to, intellectual property right (IP) violations, inaccurate or incomplete product information, incorrect product safety information, and potential environmental issues related to the products offered on the Zalando platform".*

AliExpress, 2024 DSA risk assessment report, p. 37: *"There is a risk that users may misuse the Platform functionalities to publish non-compliant content and avoid detection. This may occur through attempts to evade keyword and image detection by manipulating images and text. Additionally, abuse of the Platform's IM* [Instant messaging] *or chat features could involve the use of bots to generate spam or harass users".*

X, 2023 DSA risk assessment report, p. 28: *"*[E]*xtremist groups may circumvent controls by frequently employing coded language and updating their symbols to bypass moderation efforts, as well as obfuscating keywords and manipulating their images by cropping or adjusting colours to circumvent the automated systems that rely on such cues"* ; DSA risk assessment report 2024, p. 32: *"X's automated content detection tools for X Rules violations can act on both text and media, and those detections may or may not overlap with illegal hate speech laws in respective EU member state countries".*

Facebook, 2024 DSA risk assessment report, p. 31: *"Threat actors continue to explore ways to avoid detection and enforcement by using coded language with emojis and slurs, avoiding certain phrases, or other strategies which can make it challenging for technology to detect potential violations"* ; p. 76: *"As the types of content and terms used for hate speech are frequently changing, consistently detecting and enforcing against hate speech remains challenging. For example, threat actors continue to explore ways to circumvent detection and enforcement, such as implying instead of explicitly stating things, new trends can emerge as contentious depending on regional nuances. Additionally, often users can post content that is borderline hate speech, which makes over enforcement challenging to manage".*

3.2. Fundamental rights

Article 34(1)(b) establishes that DSA risk assessments shall include *"any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter*

and to a high-level of consumer protection enshrined in Article 38 of the Charter". This Section provides an overview of systemic risks on selected fundamental rights listed under Article 34(1)(b), on the basis of the VLOPs and VLOSEs providers' risk assessment reports and CSOs' observations.

The DSA includes safeguards against risks to fundamental rights, such as risks of negative effects on the right to freedom of expression and information. Article 35 DSA requires that providers of VLOPs and VLOSEs take mitigation measures that are reasonable, proportionate and effective. The same Article also requires that any such mitigation measures be taken with particular consideration to the impacts of such measures on fundamental rights, including the right to freedom of expression and information, as emphasised in recital 86 DSA. Other safeguards rely on transparency of content moderation, such as the requirement for providers of online platforms to give statements of reasons for content moderation decisions and to report on content moderation under Articles 15, 16 and 24 DSA. Moreover, in accordance with Article 8 DSA, both the Union and the Member States are prohibited from requiring online platforms to systematically monitor their citizens' online behaviour, which safeguards the fundamental rights to private and family life, the protection of personal data, and the freedom of expression and information.

Systemic risks related to fundamental rights have been mentioned by both providers and CSOs. The fundamental rights concerned and the risks vary across the different types of platforms. For example, the most prominent and recurrent systemic risks related to fundamental rights on online marketplaces will be different from those on social media or mapping services.

Right to freedom of expression and information.

According to its Article 1, the DSA aims to ensure a *"safe, predictable, and trusted online environment"* where fundamental rights are *"effectively protected"*, including the right to freedom of expression and information. As such, the systemic risks to the right to freedom of expression and information enshrined in Article 11 of the Charter identified by VLOPs and VLOSEs providers under the DSA's risk management framework do not concern individual pieces of content but instead the systems used to disseminate or moderate those pieces of content (e.g. recommender systems, advertisement systems, content moderation systems). Systemic risks mentioned by providers, in particular of social media and search engines, and CSOs included unjustified restrictions to users' possibilities to express themselves online and risks of lack of access to a plurality of opinions of both natural and legal persons (including media organisations).

Examples of risk factors concerning systemic risks related to the fundamental right to freedom of expression and information:

Content moderation policies and systems as well as terms and conditions: Both providers and CSOs highlighted risks related to the over-moderation of non-policy-violating and legal

content. Over-moderation may negatively affect civic discourse and create risks of negative effects on the fundamental right to freedom of expression and information. This risk factor may be exacerbated by shortcomings of appeals mechanisms for content or account restrictions, and/or due to an over-reliance on automated means of content moderation without sufficient human review, or an inadequate performance of the automated means of content moderation. Risks related to the over-moderation of content may pertain to any domain where platforms take content moderation decisions, whatever the ground may be. As such, these risks may be found across the board, regardless of whether a content moderation decision is motivated by the enforcement of a VLOP or VLOSE's terms and conditions. Some providers and CSOs also mentioned systemic risk related to the right to freedom of expression linked to systems and policies that result in the under-moderation of certain content categories, for example when failures to take down illegal hate speech discourage free expression and lead to self-censorship or other chilling effects. Changes to terms and conditions and policies have been mentioned by CSOs as having potentially an impact on content moderation systems in a way that may create or increase systemic risks under the DSA.

Intentional manipulation of the services: CSOs mentioned systemic risks related to the abuse (sometimes in coordinated attacks and other systematic ways) of mechanisms to report content in order to intimidate, silence lawful speech and discourage assembly.

Recommender systems: CSOs outlined that recommender systems may affect risks that are more likely and more severe for specific populations. For example, the fact that content from certain specific groups (e.g. people with a disability, religious or ethnic minorities) may not be recommended, or be less recommended than others. Some providers remarked that systemic risks resulting from recommender systems may be largely similar regardless of where the recommendations appear (e.g. homepage, feeds).

Examples of observations concerning systemic risks related to the fundamental right to freedom of expression and information:

Wikipedia, 2023-2024 DSA risk assessment report: *"User-to-user interactions on Wikipedia could cause distress or other emotional harms to targeted individuals or groups (youth; women; racial, ethnic, or linguistic minorities; LGBTQIA+ individuals; persons with disabilities; etc.) in such a way that their participation in Wikipedia projects is deterred and their freedom of expression and contributions to knowledge equity are diminished".*

X, 2024 DSA risk assessment report, p. 42: *"Abuse and harassment, hateful conduct, violent speech and privacy violations can result in risks to freedom of expression, through harms such as censorship resulting from enforcement of platform policies as well as self-censorship from users who experience abuse and harassment on the platform".*

Non-discrimination. Systemic risks to the fundamental right to non-discrimination enshrined in Article 21 of the Charter have been mentioned in the risk assessment reports of VLOPs and VLOSEs providers, in particular social media and search engines, highlighting systemic risks stemming from the large-scale dissemination and amplification of content that may reinforce discriminatory views. Specific risks of discrimination have been mentioned by providers and CSOs and resulting from the promotion of stereotypes, discriminatory statements and biases against specific groups based in particular on their gender, racial, ethnic or cultural origin, religion or belief, disability, age or sexual orientation.

Examples of risk factors concerning systemic risks related to the fundamental right to non-discrimination:

Advertising systems: The facilitation of the presentation of advertisements in a discriminatory manner, such as targeting the presentation of advertisements with job vacancies exclusively to people of a certain gender has been mentioned by providers and CSOs.

Recommender systems: CSOs have also published research suggesting that algorithmic amplification may benefit certain groups while excluding others.

Examples of observations concerning systemic risks related to the fundamental right to non-discrimination:

Booking, 2024 risk assessment report, p. 18, mentioned that *"content moderation and discrimination detection systems may well have some limitations due to the difficulties in detecting certain types of discriminatory content (e.g., local dialects or symbols)"*.

Google, 2024 risk assessment report, p. 133, mentioned risks that *"an application or service is not of adequate quality across languages, markets and age groups* (…) [or] *does not function equitably for users with disabilities"*.

Bing, 2024 risk assessment report, p. 110, mentioned a *"risk that advertisements on Bing are biased in their targeting, affecting protected groups' ability to access critical services"* as well as a *"Risk that users leverage Image Creator from Bing or Copilot in Bing to create discriminatory or hateful content"*.

LinkedIn, 2024 risk assessment report, p. 29: *"Absent sufficient mitigations, risks related to Discrimination and Hate may manifest on the platform in ways such as members attempting to share content in Feed that contains hate speech, job posters attempting to post a job that discriminates against certain races or genders, or LinkedIn's recommender systems recommending candidates to recruiters based on bias in algorithms"*.

Rights of the child. Systemic risks to the rights of the child enshrined in article 24 of the Charter that were identified concerned mainly child safety and the protection of minors, which are presented in detail in Section 3.4 below.

Consumer protection. In addition to the systemic risks to consumer protection related to illegal content mentioned in Section 3.1, other related systemic risks related to the right to consumer protection enshrined in Article 38 of the Charter have been reported by providers of VLOPs and VLOSEs and CSOs/ These concerned for example, with regard to online marketplaces, non-compliant products (e.g. products without CE marking), misleading and unfair commercial practices addictive design, fraud, scams, deceptive advertising, fake engagement, fake user reviews or the misrepresentation of business or product information. However, these systemic risks are not limited to online marketplaces. For example, CSOs highlighted the issue of cross-platforms risks of large-scale dissemination of non-compliant products arising on online marketplaces due to trends on social media promoting those products. Regarding financial scams, some social media and search engine providers as well as CSOs have identified systemic risks associated for instance with the large-scale promotion of illegal or high-risk financial products and investments, including Ponzi schemes, betting and cryptocurrencies, investments in foreign real estate or tax rebates. Other systemic risks of scams and fraud have been mentioned by CSOs for example in relation to health supplements, dating services, clairvoyance services, lotteries, gambling, giveaways and energy savings.

Examples of risk factors concerning systemic risks related to the fundamental right to consumer protection:

Advertising systems and intentional manipulation of the services: Risks of scams and fraud have been mentioned by CSOs as often resulting from deceptive advertising as well as inauthentic user reviews which lead other users to invest into the purchase of non-existing goods or non-existing financial opportunities.

Monetisation policies: CSOs noted that these risks related to advertising may be further exacerbated due to certain content monetisation policies, for example through the incentivising of clickbait content and advertisements and the targeting of vulnerable individuals (e.g. senior citizens) or the introduction of gamification features leading to compulsive shopping.

Artificial intelligence systems: CSOs mentioned that generative artificial intelligence ("AI") systems have been used in order to facilitate scams and fraud, for example by generating content impersonating public figures, such as content creators, and trusted media sources and public institutions (e.g. national banks).

Examples of observations concerning systemic risks related to the fundamental right to consumer protection:

Amazon Store, 2024 DSA risk assessment report, p. 23: *"Bad actors engage in Fake Reviews in different ways including by: employing companies or individuals directly to create fake or incentivized reviews; creating multiple fake accounts, including personal accounts, for positive review of their own products or abusive reviews of their competitors' products; taking over or compromising customer accounts to submit false reviews; and using review brokers to source reviews in order to artificially make their products look more attractive".*

Pinterest, 2023 DSA risk assessment report, p. 17: *"Unfortunately, bad actors may seek to manipulate the Pinterest platform. This includes spam attacks or bad actors using fake accounts, and there are multiple ways for this to manifest on the platform. For example, spammers may seek to make money from Pinners clicking on links that point to a spam website they own, with display ads or other monetization on the website. Or spammers may spread malware links and then monetize the network of infected devices, or spread phishing links and then monetize the stolen user credentials".*

What To Fix, submissions to the invitation for contributions from the European Board for Digital services and the European Commission, p. 1: *"Monetization systems can have even more far-reaching consequences* [than other risk factors of Article 34(2) DSA] *by providing powerful financial incentives and channelling, or withholding access to, not only content, but financial resources".*

Rights to private and family life and data protection. Systemic Risks to the fundamental rights to private and family life and data protection enshrined in Articles 7 and 8 of the Charter have been mentioned by providers and CSOs. Situations in which users may use providers' services in order to infringe each other's rights to private and family life and data protection have been mentioned for instance in the context of surveillance applications presented for example as tools for parents to care for their children, but that are actually mainly being used to enable tracking of other individuals without their consent (this risk may also lead to gender-based violence, as addressed below in Section 3.4). Systemic risks related to stalking and doxing have also been mentioned by CSOs with regard to social media, for example concerning threats of non-consensual dissemination of intimate imagery (e.g. revenge pornography) or of other personal information (e.g. phone number, home address, government-issued ID, data concerning health).

Examples of risk factors concerning systemic risks related to the fundamental rights to private and family life and data protection:

Recommender systems and content moderation systems: CSOs noted that recommender systems optimised for engagement may contribute to the propagation of exploitative, non-consensual, or deepfake content, potentially to large audiences before content moderation systems intervene.

Intentional manipulation of the services: CSOs noted that manipulating the services of VLOPs or VLOSEs providers, in particular social media, for social engineering purposes may contribute to risks of malicious users infringing the rights to private and family life and data protection of other users.

Examples of observations concerning systemic risks related to the fundamental rights to private and family life and data protection:

Apple App Store, 2023 DSA risk assessment report, p. 39: *"Absent adequate controls, the likelihood of developers seeking to publish apps capable of giving rise to actual or foreseeable negative effects on the rights to human dignity and respect for private and family life would be high, and the severity of such risks could vary from modest to extreme (for example, in the cases of CSAM, so-called "revenge pornography", "deepfakes", etc.)"*.

Bing, 2023 DSA risk assessment report, p. 29: "[T]*he search index may enable easy retrieval of information about an individual that falls within their private sphere and that the individual did not intend or consent to make available publicly, such as non-consensual intimate imagery (NCII) (also known as "revenge porn"), or extremely sensitive personal information that could create risks of identity thefts such as credit card numbers, medical records, etc."*.

Google, 2024 DSA risk assessment report, p. 98: *"Reflecting the fact that Play exists in the app ecosystem and offers apps in categories that are likely to involve the use of personal data (e.g., banking or government services) some of the highest inherent risks for users who access content through Play relate to privacy"*.

3.3. Civic discourse, electoral processes, and public security

Article 34(1)(c) establishes that DSA risk assessments shall include *"any actual or foreseeable negative effects on civic discourse and electoral processes, and public security"*.

This Section outlines an overview of such systemic risks as identified by VLOPs and VLOSEs providers, as well as CSOs, which have particular relevance as the year 2024 was marked with

elections in many Member States including elections to the European Parliament. Article 35(1) DSA contains a broad set of examples of mitigation measures for systemic risks. Chapter 4 of this report provides an overview of existing and proposed mitigation measures. Recognising the importance of safeguarding democratic processes, in April 2024 the Commission issued guidelines under Article 35(3) DSA on *"the mitigation of systemic risks for electoral processes"*[11].

These systemic risks manifest differently depending on the nature and function of the service, the behaviours it enables, and the societal context. For example, the implications for civic discourse on social media platforms differ substantially from those on online marketplaces.

Many providers considered their handling of misinformation and disinformation when assessing potential negative effects to civic discourse, electoral processes and public security. Definitions of misinformation and disinformation vary across providers. The European Democracy Action Plan defines disinformation as *"false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm"* and misinformation as *"false or misleading content shared without harmful intent though the effects can still be harmful"*[12]. Several VLOPs and VLOSEs providers have agreed, under the Code of Practice on Disinformation, and/or its successor, the Code of Conduct on Disinformation[13], to build on these definitions. The term "disinformation" under the Code is used by the signatories to include misinformation, disinformation, information influence operations and foreign interference in the information space[14]. This report refers to the definitions of the European Democracy Action Plan when discussing disinformation and misinformation. The systemic risks outlined below relate not to individual pieces of content but to systems and processes: how services are designed, operated and used at scale.

In their risk assessment reports, when addressing systemic risks related to civic discourse, electoral process and public security, several social media platforms acknowledged the potential role of their algorithmic content recommendation systems in the viral spread of misleading narratives. With regard to negative effects on civic discourse and electoral processes, search engines focused for example on the risks that disinformation and misinformation may surface in search results due to ranking mechanisms.

---

[11] Communication from the Commission – Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277.

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0790.

[13] 2022 Code of Practice on Disinformation, available at the following link: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. The Code of Practice was converted into a Code of Conduct in 2025. The Code of Conduct on Disinformation is available at the following link: https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.

[14] Code of Conduct on Disinformation, Preamble I. a.

Systemic risks to the collective good of a well-functioning civic discourse are closely interlinked with users' fundamental rights, including the right to freedom of expression and information (see Section 3.2).

Civic discourse. Many VLOPs and VLOSE providers have reported actual or foreseeable negative effects on civic discourse as driven by the large-scale dissemination of disinformation and misinformation, including through foreign interference and information manipulation ("FIMI") campaigns, as well as coordinated inauthentic behaviour, both on and off-platform. Providers and CSOs have identified further systemic risks to civic discourse, including the suppression or lack of diversity of political content, polarisation, the spread of (violent) extremist content with the intent to radicalise users, the large-scale dissemination of harmful conspiracy theories, propaganda and falsely authoritative content (e.g. posing as official sources such as widely-recognised media organisations, public institutions or peer-reviewed research). According to providers and CSOs, such factors may contribute to polarisation and online environments detrimental to well-functioning civic discourse and democratic processes.

Voting and electoral processes. VLOPs and VLOSEs providers, alongside CSOs, have reported systemic risks to voting and electoral processes stemming from the large-scale dissemination of false or misleading content. These systemic risks may include disinformation and misinformation about election dates, candidate eligibility, voter registration processes, or the delegitimisation of democratic processes, e.g. via unfounded claims of electoral fraud, procedural flaws, interference, or institutional biases in favour or against certain persons, political parties or opinions. As also stated elsewhere in this report, the systemic risks covered by the DSA's risk management framework do not concern individual pieces of content, instead, they concern the design of the service and risks linked to how platform systems enable amplification, such as through recommendation algorithms or advertising services. Providers and CSOs also highlighted systemic risks stemming from generative AI, particularly that generative AI chatbots may answer wrongly to election-related questions, for instance by presenting wrong election dates or incorrect information about candidates.

Public figures. Several VLOPs and VLOSEs providers and CSOs have reported systemic risks related to the representation and treatment of public figures in online environments. These included the large-scale dissemination of disinformation, misinformation and harmful conspiracy theories about candidates to public office, coordinated harassment campaigns (often targeting women and minorities), impersonation, and the circulation of synthetic media designed to mislead. Providers and CSOs have noted that targets of such content typically include politicians or political candidates, civil servants, government officials, business leaders, journalists, celebrities, scientists (notably those working on climate or public health issues), and representatives of CSOs. Frequently cited examples included fabricated endorsements, false damaging admissions of misconduct or criminal behaviour, false attacks against specific individuals or groups, and falsified private communications. Providers highlighted how these systemic risks are influenced by timing, for example around elections or other significant democratic events. Certain providers and CSOs have raised concerns around users being

involuntarily exposed to political content, such as being automatically subscribed to or following political figures without their knowledge or consent.

Crises and disasters. Providers and CSOs have reported systemic risks linked to the viral dissemination of disinformation and misinformation during or following crises, whether natural or human made. Such systemic risks often manifest in real-time, when the visibility and impact of content is amplified by recommender systems and heightened user engagement. Examples cited by providers and CSOs included false or misleading narratives during floods, earthquakes, wildfires, hurricanes, landslides or industrial accidents, as well as public health crises or broader issues like climate change. The viral spreading of disinformation and misinformation has also been observed by providers and CSOs in the context of violent events, such as shootings, mass murders, terrorist attacks or armed conflicts. VLOPs and VLOSEs providers and CSOs reported cases where false claims, such as the imminent collapse of essential services (e.g. food supply chains, running water, fuel, or access to cash dispensers), may lead led to panic or hoarding behaviours. Conversely, denialism (i.e. the false claim that real crises did not occur) or the fabrication of events that never took place were also noted by some providers and CSOs as contributing to the erosion of trust in public authorities, emergency responders and scientific institutions.

Public security. Providers and CSOs have also identified systemic risks in the context of social unrest. One commonly reported risk involved the repurposing of old content, such as videos of bombings, mass shootings or large protests, framed as real-time events, with the apparent aim of triggering public panic or inflaming tensions. Providers and some CSOs have also noted systemic risks linked to the dissemination of content that praises, incites or glorifies riots, civil unrest, or criminal acts against individuals or property, including state or public infrastructure. CSOs and providers further raised concerns about risks linked to the intentional dissemination of graphic images or videos of violence, or its aftermath, in ways intended to implicitly encourage hostility or retaliation against specific individuals or minority groups.

Examples of risk factors concerning systemic risks to civic discourse, electoral processes, and public security:

Algorithmic systems, advertising systems, content moderation systems: Providers, alongside CSOs, have pointed to the role of algorithmic systems (including recommender systems and generative artificial intelligence systems), advertising systems, content moderation systems, as well as the interface designs of platforms, as relevant risk factors. For example, recommender systems may amplify conspiracy theories, propaganda, or falsely authoritative content, especially when such content mimics official or trustworthy sources (e.g. widely-recognised media organisations, public institutions, or peer-reviewed scientific research). CSOs noted that these factors may contribute to the creation of polarisation and hostile online environments, which in turn may be detrimental to well-functioning civic discourse and democratic processes. Political advertisements were mentioned by CSOs as

potential risk factors where there would be a lack of transparency about the political nature of advertisements.

Intentional manipulation of the services, virality, interface design: CSOs cited FIMI operations and other coordinated inauthentic behaviour as risk factors to civic discourse, electoral processes, and public security. The combination of sensationalism, algorithmic virality, and in some cases coordinated efforts to provoke unrest, may pose systemic risks to public security and the integrity of civic discourse, according to submissions from CSOs and providers. Some providers and CSOs explained that disinformation and misinformation e.g. in relation to electoral processes or crises may circulate in ways that disproportionately expose users to inflammatory narratives, depending on the design of the recommender system or the presence of coordinated inauthentic behaviour if recommender systems are designed to reward engagement with such content. Certain interface design features have been mentioned by providers and CSOs as potentially contributing to the rapid spread of such content, creating systemic risks to public security and institutional trust.

Examples of observations concerning systemic risks related to civic discourse, electoral processes, and public security:

Bing, 2024 DSA risk assessment report, p. 34: *"*[AI-]*Generated content could perpetuate bias, propagate false or misleading information, or contribute to echo chambers"*, and, at p. 116, mentioned a *"Risk that News promotes low authority or low quality news sources that increase political polarization and filter bubbles"*.

X, 2024 DSA risk assessment report, p. 55: *"*[E]*xternal events may result in bad actors misusing X to spread false or misleading information, as well as conduct coordinated attacks to target public security. The risk environment is heightened by the potential for echo chambers to form, where users may be exposed to information that aligns with their existing beliefs, which can reinforce biases and may stifle healthy debate"*.

Snapchat, 2023 DSA risk assessment report, at p. 130, mentioned *"The potential for personalized content and algorithmic biases lock users into echo chambers, reinforcing existing beliefs and potentially leading to polarized communities, which hinders open dialogue"*.

TikTok, 2024 DSA risk assessment report, p. 13: *"Concentrated content [footnote 5: Note that this was referred to as 'filter bubbles' in the Year 1 Report.] is a relevant risk that has been widely documented by civil society. As recommender systems are designed to offer content based on a user's interests and historical engagement, they might inadvertently present users with a narrow range of content for extended periods of time"*.

Civil Liberties Union for Europe, submissions to the invitation for contributions from the European Board for Digital Services and the European Commission: *"There is a growing concern about the inauthentic use of VLOPs and VLOSEs, where foreign actors or domestic groups intentionally manipulate the platform's systems (e.g., using fake accounts or bots, or 'buying' influencers) to influence public opinion, disrupt elections, or promote divisive rhetoric. Studies have highlighted the prevalence of coordinated inauthentic behavior (CIB) campaigns, particularly during critical political events like referenda and elections, where malicious actors aim to undermine trust in democratic processes and sow division".*

3.4. Gender-based violence, public health, protection of minors, physical and mental well-being

Article 34(1)(d) DSA requires that providers of VLOPs and VLOSEs must assess: *"any actual or foreseeable negative effects 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".* This Section outlines systemic risks identified under these categories, drawing on risk assessments of VLOPs and VLOSEs and observations from CSOs. The systemic risks in this Section may manifest differently across services, societal contexts and human behaviours. For example, minors are exposed to different risks than adults.

Gender-based violence. One of the key objectives of the EU Gender Equality Strategy 2020-2025 is to end gender-based violence ("GBV")[15]. For example, the Directive on combating violence against women and domestic violence criminalises the non-consensual sharing of intimate or manipulated material (including by means of artificial intelligence)[16]. Systemic risks related to GBV are therefore also relevant to systemic risks mentioned above in Section 3.1 on illegal content and Section 3.2 on non-discrimination. The widespread use of online intermediary services has contributed to the emergence and amplification of gender-based cyber violence. While systemic risks related to GBV were identified across all types of services, they were most frequently reported by providers of social media platforms. Providers and CSOs highlighted that GBV disproportionately affects women and girls, especially those from marginalised groups, including ethnic or religious minorities, people with disabilities, and LGBTIQ+ communities[17]. Some CSOs and providers noted that online platforms may serve as prominent channels for the amplification and normalisation of GBV and violence against marginalised groups, and that online misogyny has been referred to as a "gateway hate" that

[15] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Union of Equality: Gender Equality Strategy 2020-2025, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0152

[16] Article 5 and recital 19 of Directive (EU) of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, available at the following link: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng. It will enter into application on 14 June 2027.

[17] This was also highlighted in the Union of Equality LGBTIQ+ Equality Strategy 2026-2030, available at the following link: https://commission.europa.eu/document/download/b4952371-4308-47ad-b995-02c539b75dda_en?filename=JUST_template_comingsoon_standard.pdf.

may lead to other forms of discrimination, including LGBTIQ+ discrimination. CSOs also pointed to systemic risks such as targeted abuse based on gender. These included gender-targeted harassment, stalking, bullying, grooming, and incitement of gender-based hate.

Several providers and CSOs noted that dehumanising speech, exclusionary narratives, such as content promoting segregation and discrimination, and coordinated harassment may contribute to hostile online environments, which in turn may ultimately undermine users' freedom of expression and participation in public discourse. Some social media platform providers have also reported the specific targeting of female public figures, such as politicians, journalists and activists, which also raise concerns about the broader impact of such risks on civic discourse (see also Sections 3.2 and 3.3 on systemic risks to the fundamental right to freedom of expression and information on systemic risks to civic discourse).

Providers and CSOs also identified systemic risks related to the malicious or non-consensual sharing of personal data and sexually explicit material. This included "revenge porn", sextortion, doxing, and voyeuristic content, such as hidden camera footage and so-called "creepshots". Risk assessment reports from several providers have highlighted other instances of GBV on their services, particularly targeting women and girls, including the online promotion or facilitation of human trafficking, criminal sexual acts, coercion, manipulation, rape threats and other forms of sexualised threats and intimidation (see also Section 3.1 on systemic risks stemming from the dissemination of illegal content).

Examples of risk factors concerning systemic risks related to gender-based violence:

Content moderation systems and recommender systems: Content moderation systems and recommender systems were frequently cited by providers and CSOs as playing a role in shaping user exposure to and amplification of GBV-related content.

Artificial intelligence systems: The use of AI-generated content to facilitate the non-consensual creation, manipulation, or dissemination of explicit material, including sexual acts or deepfake pornography, has also been mentioned by CSOs as a growing concern, since it may disproportionately target women in public life and may often be deployed in the context of broader disinformation and misinformation, (sexual) harassment, intimidation or reputational harm campaigns.

Examples of observations concerning systemic risks related to gender-based violence:

Save the Children Denmark, submissions to the invitation for contributions from the European Board for Digital Services and the European Commission: *"*[G]*irls are more often negatively affected by having their private or intimate photos or videos shared than boys"*.

Google, 2024 DSA risk assessment report, p. 55, mentioned the following risks: *"Image-based abuse, including content created using generative AI tools (such as CSAM, NCEI* [Non-Consensual Explicit Images]*, and ISPI* [Involuntary Synthetic Pornographic Images]*) and gender-based/LGBTQIA+ harassment, hate, and bullying"*.

Instagram, 2024 DSA risk assessment report, p. 66: *"We also recognise that LGBTQIA+ community as well as public figures like female politicians, especially female politicians of colour, are targets of bullying and harassment at a disproportionate rate. This can cause silencing of the LGBTQIA+ community and women's voices and intimidation and/or fear for their safety"*.

***Public health*.** Providers and CSOs noted systemic risks to public health stemming from the large-scale dissemination of disinformation or misinformation on social media and search engines. These concerned for example vaccines, misleading claims about legal but potentially harmful substances and practices, the gamification of viral harmful health trends, or serious medical conditions such as Ebola, HIV/AIDS or diabetes. Providers of online marketplaces noted related systemic risks stemming from the sale of illegal, non-compliant, or unregulated medical products on their marketplaces. Examples included the sale of counterfeit or substandard medical products (e.g. uncertified face masks), as well as the sale of unauthorised/unlicenced medical devices, supplements or pharmaceuticals (e.g. weight loss drugs). Providers also mentioned systemic risks linked to the promotion of legal but harmful substances, such as alcohol, tobacco, and prescription drugs, and content linked to self-harm, eating disorders or risky health practices. In certain cases, providers and CSOs have further identified systemic risks related to large-scale coordinated health disinformation and misinformation and manipulated media used for economic or political purposes. Section 3.3 examines issues related to disinformation and misinformation in more detail in the context of systemic risks to civic discourse, elections and public security.

Examples of risk factors concerning systemic risks related to public health:

Advertising systems and other risk factors: Risk factors contributing to the dissemination and amplification of public health risks such as platform design, features and interfaces, content moderation systems and recommender systems have also been mentioned by providers and CSOs. With regard to advertising systems specifically, CSOs mentioned systemic risks related to influencer marketing promoting scams or unsafe products, with minors being particularly vulnerable as they may struggle to recognise the commercial nature of influencer promotions, even when disclaimers are present.

Examples of observations concerning systemic risks related to public health:

Bing, 2024 DSA risk assessment report, p. 127, mentioned the existence of a *"Risk that Search results include information about medical conditions, treatments, vaccines, or homeopathic remedies that are inaccurate, unsafe, or otherwise not appropriate or advisable based on an individual's condition"*.

European Fact-Checking Standards Network, submissions to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Health misinformation remains a persistent and highly damaging systemic risk across the EU, with widespread examples of false or misleading content circulating on Very Large Online Platforms (VLOPs). Health misinformation can cause significant harm to individuals but also in cases of public health emergencies"*.

Fundacion Maldita, submissions to the invitation for contributions from the European Board for Digital Services and the European Commission: *"An important aspect of medical disinformation is its frequent link to monetization.* (…) [F]*raudulent endorsements exploit the perceived authority of medical professionals to persuade users into purchasing potentially harmful treatments or supplements.* (…) *Certain content subtly or overtly encourages disordered eating habits, glamorizing extreme dieting and unhealthy body image standards. Given the vulnerability of this demographic, such content can contribute to serious mental and physical health issues"*.

Protection of minors. Most VLOPs and VLOSEs providers, in particular social media platforms and search engines, as well as CSOs have mentioned systemic risks related to the protection of minors. These included for example the presence and distribution of CSAM, sexualisation of minors, sextortion, grooming, cyberbullying, the promotion of self-harm, child trafficking and exploitation, and other inappropriate adult-minor interactions, particularly in environments that enable anonymous or private interactions. The excessive, compulsive, addiction-like use of social media has also been mentioned by providers and CSOs, as detailed in the paragraph below on systemic risks to mental well-being. Specific systemic risks have also been noted by CSOs regarding the commercial exploitation of minors as influencers, including by their parents or guardians. Some providers and CSOs mentioned issues of inclusivity, citing a lack of quality content across languages and inadequate accessibility for children with learning challenges or disabilities. Some CSOs also mentioned risks that minors may not trust reporting mechanisms for harmful content, and/or that these mechanisms are not child-friendly, which may contribute to an under-reporting of issues. Although social media and search engines are highlighted by CSOs as the main types of platforms for systemic risks to the protection of minors, some CSOs mentioned that the use of other types of platforms such as online marketplaces may also carry risks, for example due to misleading marketing methods that adults may recognise but not minors. Systemic risks related to the use of social media for

the recruitment of minors for organised crime or terrorism have also been identified[18]. Additionally, providers have reported systemic risks related to the exposure to violent content, social media, and live-streaming environments, (peer-to-peer) bullying, harassment, targeted abuse, stalking, doxing, child non-sexual abuse. Harmful social media challenges have also been mentioned by providers and CSOs as systemic risks.

Examples of risk factors concerning systemic risks related to the protection of minors:

Recommender systems: Recommender systems were noted by providers and CSOs for their potential to amplify the dissemination of harmful content (e.g. legal but potentially problematic or content being algorithmically recommended to child users with increasing frequency and thus becoming harmful for its cumulative effect).

Artificial intelligence systems: CSOs mentioned the increasing use of generative AI systems to create CSAM content from any picture or video of a child, and its subsequent dissemination via VLOPs and VLOSEs, as well as systemic risks related to generative AI chatbots (e.g. with which children may create an emotional attachment which may disrupt their relational development).

Intentional manipulation of the services: Risk assessment reports of providers highlighted concerns about adults posing as minors, creating fake profiles, or sharing accounts with children. Providers have reported challenges in age assurance, where guardians misunderstand or mismanage age-verification processes or minors bypass verification or estimation measures by misstating their age, or where minors purchase or share fake accounts. Similarly, they noted challenges in content moderation, for example with the use of coded language and emojis to evade moderation that changes frequently (e.g. "chicken soup" referring to self-harm, "cheese pizza" referring to CSAM). Risk assessment reports also noted instances of children being moved/redirected off-platform towards less moderated or offline spaces, increasing risks of exploitation.

Examples of observations concerning systemic risks related to the protection of minors:

TikTok, 2023 DSA risk assessment report, p. 16, mentioned the existence of the following risk in relation to the protection of minors: *"'Conduct Risk' and 'Contact Risk': In creating and posting content on the Platform, or by engaging with content posted by others, minors*

[18] European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE), 4 June 2025 hearing on *"Radicalisation online, with a focus on the recruitment of children for organised crime and terrorism"*, available at the following link: https://www.europarl.europa.eu/committees/en/online-radicalisation-recruitment-of-chi/product-details/20250516CHE13127. Europol Intelligence Notification of 20 February 2025 on *"The rise of online cult communities dedicated to extremely violent child abuse"*, available at the following link: https://www.europol.europa.eu/publications-events/publications/rise-of-online-cult-communities-dedicated-to-extremely-violent-child-abuse.

may engage in inappropriate behaviour or potentially encounter inappropriate behaviour from other users, such as inappropriate comments, bullying or behaviour amounting to child sexual exploitation".

Eurochild, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Another influencing factor, identified by some VLOPs in their reports, is Artificial Intelligence, especially content generators. Despite still an evolving field, the generation of harmful material with AI-powered technologies is an increasing trend. This is especially dangerous when used for child sexual abuse, including grooming sexual extortion and the creation of AI-generated CSAM – through not only fine-tuned models but also general-purpose AI systems. Two additional concerning trends have emerged: (1) AI-generated results reinforcing harmful stereotypes, disproportionately affecting vulnerable children; and (2) the emotional manipulation of children through AI chatbots and companions"*.

Knight-Georgetown Institute and **Panoptykon Foundation**, joint submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Platform design plays an important role in creating risks of unwanted and harmful contact. Some platforms, for example, enable user visibility by default and recommend user accounts to others outside their network, as well as accounts outside a user's network to them. These designs pose particular risks to minors by enabling bad actors to target and/or mass contact minors' accounts. Research has found that expansive default account visibility and account recommendations are crucial design vulnerabilities for sextortion targeting minors"*.

Physical and mental well-being.

- ***Physical well-being.*** Systemic risks to physical well-being have been identified in relation to different types of providers. For example, providers and CSOs highlighted systemic risks on social media concerning suicide, self-injury, unrealistic body standards, eating disorders, extreme weight loss, incorrect or harmful recovery strategies against eating disorders or drug use without appropriate restrictions or disclaimers. In contrast, online marketplaces have primarily highlighted systemic risks associated with harmful goods and services, such as physical products that may cause allergic reactions or accidents. Sections 3.1 and 3.2 examine related issues in more detail together with other systemic risks related to the dissemination of illegal content and to consumer protection. Providers and CSOs also mentioned systemic risks from application stores with apps that may encourage harmful behaviours, spread health disinformation or misinformation, or target vulnerable users with deceptive content. Excessive screentime has been associated with potential physical well-being risks such as myopia and strain on eyesight by researchers. Some providers and CSOs have described how users, in particular minors, may, as a result of excessive use, displace essential activities like sleep and exercise, and in-person social interactions, and how

such behaviours may show similarities to mechanisms observed in gambling and substance use disorders, potentially resulting in negative effects on their physical health.

- ***Mental well-being.*** Providers have identified systemic risks to mental health and well-being, in particular stemming from the exposure to certain types of content and from excessive, compulsive, and addiction-like use of social media and compulsive buying disorders on online marketplaces. CSOs have underlined the exposure to certain content as an important mental health risk, particularly for vulnerable users, such as marginalised groups or minors. Risk assessment reports have noted that content related to self-harm, suicide, and eating disorders may contribute to the normalisation or encouragement of harmful behaviours in users. Some providers have highlighted the additional systemic risk stemming from prolonged exposure to harmful content, which may lead to sustained psychological distress in users, citing examples such as targeted harassment, cyber bullying, and insults, particularly based on certain characteristics of an individual or a group. Some CSOs mentioned systemic risks of anxiety related to a high exposure to news content on social media, for example in relation to armed conflicts.

Examples of risk factors concerning systemic risks related to physical and mental well-being:

Designs, interfaces, features: Providers and CSOs have identified mental and physical health risks associated with the design and use of VLOPs and VLOSEs, particularly in relation to excessive, compulsive and addiction-like use of social media. Some noted the role of platform design features, such as infinite scroll, autoplay, ephemeral content, notifications and other interface elements linked to patterns of compulsive use, particularly when platforms encourage engagement without significant user control (e.g. disengagement mechanisms). Several CSOs mentioned that such features and designs may be highly addictive. Other CSOs noted systemic risks related to platform designs set to maximise time spent on an app or nudge users to act in certain ways as to gain attention and validation. For example, some CSOs noted that gambling-like and addictive features in video games available on or advertised on platforms may also lead to risks, in particular for minors and vulnerable individuals. Features such as beauty filters have been mentioned by CSOs as contributing to users' negatively perceiving their own body images and promoting unrealistic social comparisons.

Recommender systems and artificial intelligence systems: Furthermore, CSOs and providers have mentioned that these issues may be exacerbated by the so-called "rabbit hole effect", whereby specific types of content are repeatedly recommended. Likewise, some CSOs mentioned how content that may not be harmful to the general population or that may not be problematic when seen in isolation may create risks if it seen (repeatedly) by vulnerable individuals (e.g. minors, people suffering from addictions or illnesses). Systemic

risks to physical and mental well-being from the use of generative AI chatbots have also been mentioned by CSOs, for example in the context of the recommendation of harmful health advice (e.g. in relation to eating disorders), in particular for children.

Examples of observations concerning systemic risks related to physical and mental well-being:

Snapchat, 2023 DSA risk assessment report, p. 190, under the header "Filter bubble": *"There is a risk therefore that, without safeguards, the algorithm will tag users who view content that may not be harmful on its own as being interested in that content and that repeated and frequent exposure to that content could be harmful".*

Instagram, 2024 DSA risk assessment report, p. 66: *"Bullying and Harassment is associated with the Civic Discourse and Elections, Gender-based Violence, and Protection of Minors Systemic Risk Areas in the DSA. This Problem Area refers to the risk of Meta's systems being used to promote content that degrades or shames users or to make repeated contact with a user that is unwanted, such as cyberbullying, threats of harm, mass harassment, and sexual harassment. We recognise that bullying and harassment can have disproportionate effects on minors' well-being and mental health".*

TikTok, 2024 DSA risk assessment report, p. 50, under the headings *"Risks related to AIGC* [AI-Generated Content]*"* and *"Well-being impact and social comparison": "Early research indicates there are risks to Younger Users' well-being associated with AIGC, including content created using off-platform AIGC tools, in particular around self-esteem, body image, and mental health".*

Google, 2024 DSA risk assessment report, p. 134, mentioned the existence of a *"*[R]*isk that the interface, design, or features of a service stimulate compulsive use of the service for users, including children".*

Knight-Georgetown Institute and **Panoptykon Foundation**, joint submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"To deliver hyper-personalized experiences, social media recommender systems may rely on behavioural patterns. These patterns may reveal individual vulnerabilities such as addictions, eating disorders, body complexes, anxiety, or depressive disorders. Recommender systems designed to maximize user engagement may purposefully or inadvertently exploit or exacerbate these individual vulnerabilities. Depending on the individual, these systems can also create feedback loops that drive users into narrower selections of content, corresponding to their vulnerabilities. Such content may not be dangerous per se, and may be entirely acceptable when considered in isolation, but becomes harmful if consumed consistently over time by vulnerable individuals".*

4. Practices to mitigate systemic risks

This Chapter essentially follows the structure of Article 35(1) DSA in presenting an overview of the main categories of measures mentioned by providers and CSOs to mitigate systemic risks. Each Section of this Chapter corresponds to one or several sub-paragraphs of Article 35(1), except for Article 35(1)(j) which does not have a dedicated Section because mitigation measures related to the rights of the child are presented throughout the others.

Article 35(2) states that the Board report *"shall include* (…) *best practices for providers of very large online platforms and of very large online search engines to mitigate the systemic risks identified"*. The DSA is still at an early stage of its implementation, including of Articles 34 and 35, and, as such, this first edition of the Board report therefore consists of a presentation of current practices and practices proposed by providers or CSOs without singling any out as "best" or necessarily even "good" practices and which is by its very nature incomplete. Besides, and as stated in Chapter 1, nothing in this report should be interpreted as guidance for the compliance with Articles 34 or 35 DSA and nothing in this report should be interpreted as constituting an assessment or evaluation of compliance by designated VLOPs and VLOSEs with Articles 34 or 35 DSA, or any other provision of the DSA. This report is without prejudice to any current or future investigations, enforcement actions, or formal findings under the DSA framework.

Furthermore, the practices presented in this report should not be considered in isolation, instead, they should be looked at as potential elements for combinations of measures to ensure the mitigation of specific risks. As highlighted in Chapter 1, providers should have particular consideration for the impacts of such measures on fundamental rights, including the right to freedom of expression and information.

VLOPs and VLOSEs providers may have adopted certain risk management measures, possibly even before the entry into application of the DSA, that contribute to mitigating systemic risks under the DSA, for example as part of running of their business, or compliance with other applicable laws. For example, all providers have detailed and extensive terms and conditions governing their use, and most if not all online platforms have had some form of content moderation measures in place even before the entry into application of the DSA. One novelty introduced by the DSA is the requirement to report comprehensively on the risk assessments performed and subsequent mitigation measures adopted, thereby increasing transparency around systemic risks and their mitigation. Providers of VLOPs and VLOSEs are required to put in place effective mitigation measures pursuant to Article 35(1) DSA, under the supervision of the Commission, and to report on them publicly pursuant to Article 42(4) DSA, so that anyone may obtain information about those measures. This permits accountability and outside scrutiny for VLOPs and VLOSEs providers that adds to regulators' role. Systemic risks are evolving over time, this is why the DSA's risk management framework requires a constant renewal of both risk assessment and mitigation measures. It is in light of this regular succession of risk management activities required from the providers that the Article 35(2) reports of the

Board, in cooperation with the Commission, will enable a yearly transparency and stocktaking exercise.

The consultations and input gathered in preparation for this report highlighted that, in order to enable VLOPs and VLOSEs providers and CSOs to best identify mitigations going forward, VLOPs and VLOSEs providers need to ensure a meaningful involvement of representatives of users, affected groups, CSOs and researchers during the preparation of the risk assessment reports. The remarks on recital 90 of the DSA from Chapter 1 and from the introduction to Chapter 3 above are thus also relevant with regard to the identification of reasonable, proportionate and effective mitigation measures.

Lastly, this report recalls the importance of the Commission Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065[19], the Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065[20], as well as the Code of Conduct on Disinformation[21] and the revised Code of Conduct on countering illegal hate speech online[22], but does not elaborate or provide an evaluation of the uptake of such measures adopted by providers. Likewise, this Chapter does not elaborate on measures undertaken as part of compliance with other acts of Union law.

4.1. Design, features and functioning of the services, including online interfaces

Article 35(1)(a) DSA refers to the following mitigation measures for providers to put in place: *"adapting the design, features or functioning of their services, including their online interfaces"*.

In their reports, many providers outlined measures to mitigate systemic risks stemming from the design, features, or interfaces of their systems. For example, some providers of online marketplaces indicated that they mitigate systemic risks by limiting social functionalities and user interactions (e.g. chat between users), restricting the dissemination of user-generated content, or content personalisation by default. To mitigate systemic risks stemming from the dissemination of certain categories of content, including both illegal content and content that may give rise to risks falling into the other risk categories in Article 34 DSA, CSOs suggested introducing nudges, friction-inducing elements such as circuit breakers, for instance to remind users of certain rules before posting content (see also Section 4.4 on recommender systems). Furthermore, some CSO suggested that providers should not rely on potentially addictive

[19] Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, available at the following link: https://eur-lex.europa.eu/eli/C/2025/5519/oj/eng.
[20] See footnote 11.
[21] See footnote 13.
[22] The 2025 revised Code of conduct on countering illegal hate speech online, available at the following link: https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online.

design features, for example by turning off features such as notifications and autoplay by default. Blurring images and videos have been mentioned by several providers and CSOs as a mitigation measure for certain types of harmful content (e.g. containing violence), including blurs accompanied by warning messages (e.g. in direct messages, to warn users not to feel pressured to reply to messages containing nudity content, especially when received without solicitation). Blocking features and other mechanisms to prevent other users from seeing or interacting with one's content or controlling the conditions according to which others may see or interact with one's content have been mentioned by providers and CSOs. Some CSOs and providers mentioned the importance for the providers to retain information after a user has been blocked, in particular for the purpose of preserving evidence of past conversations in case of investigations (e.g. into harassment).

Providers, particularly those of social media platforms, and CSOs have highlighted various design decisions or default settings to protect minors. These included for example awareness raising measures such as disclaimers on legal age requirements and articles in online safety centres, limiting live streams and access to AI features to adult users, making educational content feeds easier to discover, utilising content classifiers based on the appropriateness of the content for different age groups, and making minors' accounts private by default to limit interactions with potentially harmful users. Most search engines mentioned safe search functionalities turned on by default for minors, to filter out search results that the provider classifies as inappropriate for minors. Some providers mentioned reminders (e.g. to go to bed or take a break from watching content) tailored to different age groups. Additionally, some providers have put in place parental control tools offering specific settings, to help guardians manage children's online experiences. Some of the parental control tools mentioned ranged from enabling parents to set daily limits for app usage to providing notifications about their children's screen time, reporting behaviour and online connections. In some cases, providers mentioned disabling the infinite scroll and autoplay functions by default for minors. Some CSOs suggested introducing a safety by design approach to better protect minors, including the use of specific labels for content made for minors and dedicated classifiers for such content. CSOs mentioned the identification and limitation of repeatedly recommended types of content to minors.

4.2. Terms and conditions and their enforcement

Article 35(1)(b) DSA refers to the following mitigation measures for providers to put in place: *"adapting their terms and conditions and their enforcement"*[23].

All providers reported that they regularly monitor and update their terms and conditions to address emerging and evolving systemic risks (e.g. deepfakes), new user trends (e.g. repeated

[23] The Commission created a Digital Services Terms and Conditions Database, which is available at the following link: https://platform-contracts.digital-strategy.ec.europa.eu/.

violations by users), changing legal requirements (e.g. new national legal frameworks), or other developments (e.g. new design features).

Regarding minors, some providers stated having introduced provisions in their terms and conditions that restrict minors from accessing their services, registering accounts, or using payment methods. Some providers also claimed to conduct regular age verification checks to ensure enforcement of their terms and conditions. Some providers stated that they enhanced their terms and conditions by including cases, examples, or illustrations to make them more concrete and understandable.

4.3. Content moderation systems

Article 35(1)(c) DSA refers to the following mitigation measures for providers to put in place: *"adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation".*

Tools and methods of content moderation. Providers mentioned combinations of pro-active content moderation methods (by the providers themselves, with both automated and human reviews) and re-active methods (upon user reports). Providers and CSOs mentioned the use of AI in content moderation, highlighting both its advantages (e.g. scale, speed of reaction) and shortcomings (e.g. with regard to the explainability of decisions), and that, as such, it may both represent a risk factor and a mitigation measure. CSOs highlighted the importance of having sufficiently resourced content moderation teams to cover a broad range of languages.

Furthermore, CSOs emphasised the need for human moderators to be well trained and also aware of local contexts, languages and cultures. For example, some providers mentioned mitigation measures to detect when certain emojis are used as code to conceal illegal activities, such as the sale of illegal drugs. Some providers also mentioned the creation of early detection models to identify dangerous viral trends, such as harmful challenges. The use of wordlists has been mentioned (including anti-circumvention measures to adapt to new slang terms and the use of emojis, especially for content posted by minors, and early detection models to identify new trends such as dangerous challenges). Similarly, the use of fingerprints/content hash matches have been highlighted for illegal content (e.g. terrorist content, CSAM, intellectual property rights violations). The use of automated transcriptions of audio into text, and the automated analysis of the resulting text has also been mentioned by some providers as a way to improve content moderation. The use of human reviews for content reaching certain thresholds of popularity has also been mentioned by some providers. The use of content filters based on age for minors has also been mentioned (e.g. different filters for suspected under 13 users, for users between 13 and 15, for users between 16 and 18). Contextual text moderation measures have also been referred to (e.g. explaining to users why certain content/comments may not be

posted due to being caught by content moderation filters). The need to ensure consistency of content moderation across formats (e.g. text, images, videos) and surfaces (including live streams) has been mentioned by providers. The collaboration with independent fact-checkers has been highlighted by providers and CSOs, in particular in the context of the Code of Conduct on Disinformation. The use of community notes has also been mentioned by some providers and CSOs.

At an operational level, there have been mentions of the importance of having close links between content moderation and legal teams to escalate borderline cases, as well as partnerships with anti-bias researchers and CSOs and the establishment of market-specific moderation processes to capture local nuances in languages, slang terms and cultural references (in particular in the context of hate speech), and ensuring consistency of content moderation enforcement by human reviewers 24/7 (e.g. by taking advantage of time zone differences). The importance of taking off-platform and offline events into consideration has been highlighted by CSOs in order to anticipate moderation challenges spreading from one platform to another. Many providers mentioned having channels of communication with law enforcement authorities, for example with regard to illegal content such as CSAM. The regular performance of internal and external audits and reviews of content moderation policies and enforcement, as well as assessments of how other legal obligations than the DSA may impact their moderation practices (e.g. General Data Protection Regulation[24]) have also been described by some providers.

In terms of penalties for users posting content regularly moderated, escalation mechanisms ranging from warnings to demonetisation and platform removals have been mentioned by providers. The off-platform behaviour of certain users has been highlighted as part of the factors to take into account in moderation decisions by some providers.

Topics of moderation. The topics most commonly referred to concerning content moderation were anything listed as illegal content and services, as well as content violating terms and conditions, such as for example age-inappropriate content, slurs, bullying and harassment, discriminatory behaviour, content from dangerous organisations and criminals, inauthentic behaviour and platforms manipulations.

The existence of derogations from moderation for content that would have otherwise violated terms and conditions (e.g. violence, armed conflicts) has been mentioned by several providers if that content has specific value, for example educational, documentary, scientific, satirical or artistic. Some providers mentioned additional controls and designs for child safety, including specific filters for parents and guardians to control the content their children may see.

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at the following link: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

In the context of content moderation of illegal products on online marketplaces, such as IP infringing products, non-compliant and hazardous goods, providers have mentioned automated and semi-automated content moderation practices such as monitoring and screening tools, cross-checking products with a high level of similarity to previously removed products, systems to identify products with confirmed non-compliance/illegality. Providers also mentioned the conduct of own-initiative product compliance checks including with third-party laboratories. Several mitigation measures are directed towards traders, such as measures designed to increase the knowledge of traders on Union product regulations, or incentive initiatives such as the sanctioning or blacklisting of traders selling illegal products. In the area of counterfeit and IP infringing products, platforms such as online marketplaces mentioned collaborations with right holders through IP/brand protection programmes for example to identify counterfeit products hiding behind fake listings as well as other kinds of abuses. Some VLOPs and VLOSEs providers furthermore reported offering specialised tools for brands to manage and protect their rights, including features for cross-platform searching, image blocking, and bulk enforcement actions.

With regard to content from sanctioned entities, CSOs suggested measures such as geo-blocking, demonetisation, shadow banning or outright bans for users and accounts disseminating content from sanctioned entities. In this context, CSOs also suggested regular reviews of sanctions lists by VLOPs and VLOSEs providers.

4.4. Algorithmic systems including recommender systems

Article 35(1)(d) DSA refers to the following mitigation measures for providers to put in place: *"testing and adapting their algorithmic systems, including their recommender systems"*.

Content recommendations. Providers and CSOs reported that harmful or potentially harmful content, such as illegal content, inauthentic content, content from repeat violators of terms and conditions, or disinformation, may be demoted by recommender systems. In some cases, providers and CSOs mentioned that the dissemination of content may be restricted, for example, for content created by minors or content that has reached a certain level of popularity but has not yet undergone human review. Similarly, providers noted that content on high-risk topics or during critical periods, such as elections, or crises such as natural disasters or public health crises may be restricted from dissemination. Some providers reported observing spillovers from offline coordination or incidents from other platforms, such as viral trends, and using information banners or interstitials to limit the spread of such content.

Design of systems. Some providers claimed that their algorithmic systems are designed to recommend content that is diverse, not narrow or repetitive, and that content items curated for potential recommendation are sourced from reliable sources and trusted experts. Some providers claimed that their recommender systems do not optimise for view time only but also for content quality. Providers and CSOs remarked that recommender systems as well as content moderation systems may be considered not only as risk factors but also as risk mitigation

measures to the extent that they may promote authoritative content. Certain CSOs suggested implementing functionalities that foster the visibility of marginalised voices and content. Benefits from recommender systems that are not predominantly based on user engagement have been mentioned by both CSOs and some providers; for example, some CSOs mentioned potential mitigation measures such as bridging (i.e. focusing recommendations on content promoting productive dialogue or positive emotions). Some CSOs mentioned that the monetisation policies of certain providers may amplify the dissemination of harmful content through recommendations and that increasing transparency about those policies might act as a mitigation measure.

User choices. Some providers explained giving users the option to reset their recommendation profile to emulate a new user or allow them to turn off or opt out of recommender systems. Some providers mentioned allowing users to indicate that they are "not interested" in specific content, signalling to the systems to reduce exposure to similar content. Moreover, some providers explained permitting users to select keywords for content display or filtering. Certain providers also presented the use of notices to help users understand why certain content is recommended to them. Certain CSOs mentioned that tools for users to explicitly state which type of content they would like to get recommended may help mitigate certain risk, for example, surveys of users' preferences, including preferences for long- or short-form content, as well as the ability to activate "hard stops" to prevent the display of certain types of content.

For minors, some providers explained having implemented additional safeguards, for example for the recommendation of potential friends or connections, or for showing content that is more suitable for their age. CSOs have proposed to limit interactions with unknown users by default, for instance to limit the ability for strangers to contact minors via direct messages. For verified minor accounts, some CSO suggested developing separate recommendation algorithms prioritising age-appropriate content.

4.5. Advertising systems

Article 35(1)(e) DSA refers to the following mitigation measures for providers to put in place: *"adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide"*.

Providers mentioned mitigation measures for their advertisement systems such as: vetting processes for advertisers (e.g. only vetted CSOs being allowed to publish advertisement on certain sensitive topics such as armed conflicts), the pre-screening of advertisements before their publication (including specific controls for advertisements that may promote scams, fraud, illegal content and services or medical disinformation, as well as products such as alcohol and tobacco). Some providers mentioned using audience minimums for advertising systems not to perform too narrow targeting. Some providers mentioned the prohibition of advertisements containing AI-generated content about sensitive topics such as elections, as well as self-declarations by advertisers about the use of AI in the creation of an advertisement.

In terms of penalties for violation of the advertising policies, removal of the advertisement from the platform has been mentioned by providers. Training and information for influencers concerning risks of violating advertising laws has also been mentioned by CSOs, including about the possibility in some Member States to seek training certificates from advertising regulators. Many providers stated that they do not enable direct advertising to minors based on personal data and that they offer options for minors to opt out of personalised recommendations. To keep the focus of this report on the DSA, rules set out in other pieces of Union legislation concerning advertising, such as the Regulation on Transparency and Targeting of Political Advertising[25], are not discussed here with regard to potential mitigation measures.

4.6. Risk detection and challenges related to the misuse of the services, content and account authenticity

Article 35(1)(f) DSA refers to the following mitigation measures for providers to put in place: *"reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk"*.

Article 35(1)(k) DSA refers to the following mitigation measures for providers to put in place: *"ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information"*.

Tools and methods of risk detection. In order to detect systemic risks of misuse of their services and issues related to the authenticity of content (e.g. deepfakes) and accounts (e.g. bots), providers and CSOs mentioned a host of mitigation measures. For example, some providers mentioned the reliance on content, behavioural and technical signals to detect inauthentic behaviour (e.g. patterns in the speed of content sharing that would seem implausible for a human to perform). These in certain cases were described as involving AI to detect content created by AI (as well as creating policies to prevent the use of AI to impersonate others, including public figures, or to generate medical or legal advice). Some providers explained keeping an index of fake or compromised accounts and having established measures to prevent banned users from rejoining the platform under different aliases or through intermediaries. In the same vein, the use of third-party and open-source hashes and keywords databases for signals on upcoming threats has also been mentioned. Some CSOs suggested that AI-enabled systems could match content with databases and trusted news sources to identify false claims quickly and in a scalable way, and to help facilitate the work of fact-checkers. Measures to prevent

[25] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, available at the following link: https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng.

signposting (i.e. content that leads off-platform to circumvent terms and conditions enforcement) have been described by certain providers.

Some providers and CSOs mentioned staggered rollouts of new features and designs as a mitigation measure, including with the use of holdout/control groups (i.e. groups of users to whom new features or designs are not immediately available, potentially for prolonged periods) serving as comparison with the rest of the user base in order to help isolate and identify potential new risks for instance when A/B testing new features.

Operational risk detection. Some providers described the establishment of threat detection teams (including with expertise concerning FIMI and cutting across functions, e.g. legal, trust and safety, cyber-intelligence, finance and anti-money laundering), with linguistic capabilities to understand local threat landscapes. In this context, the use of "red team" approaches has been mentioned by certain providers. There have also been mentions of the importance of direct channels of communication with CSOs and public authorities, as well as the conducting of post-mortem/lessons learned exercises after important events such as elections or crises, and the publication of regular threat reports on platforms manipulation. Some CSOs suggested working directly with affected communities and involving them in finding suitable mitigation measures for identified risks.

Account verification. Providers and CSOs also mentioned the importance of account verification as a way to prevent platforms manipulations, including two-factor authentication, the deletion of accounts of users below 13 years of age, and programmes such as "know your developer" for application stores. Providers have noted the (re)allocation of resources for monitoring and enforcing their terms and conditions, such as implementing mechanisms to prevent circumvention or coordinated attacks by bad actors. In this context, some providers, particularly online marketplaces, explained requiring, in some cases, two-factor authentication for third parties to use their services and/or publish content.

4.7. Trusted flaggers

Article 35(1)(g) DSA refers to the following mitigation measures for providers to put in place: *"initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 and the implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21"*.

Some providers mentioned the compilation of reports from trusted flaggers, the involvement of trusted flaggers in their product safety development processes and product updates, the creating of dashboards for trusted flaggers to follow-up on the status of their notices, the creation of partnerships with CSOs and public authorities to perform similar roles as trusted flaggers and report e.g. suspected illegal content.

4.8. Codes of conduct

Article 35(1)(h) DSA refers to the following mitigation measures for providers to put in place: *"initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively"*.

The DSA gives a special role to Codes of Conduct to present industry best practices to mitigate systemic risks. VLOPs and VLOPEs providers are encouraged to cooperate with one another, including by joining Codes of Conduct. Some providers made references to Codes of Conduct such as the Code of Conduct on Countering Illegal Hate Speech Online and the Code of Conduct on Disinformation (formerly Code of Practice on Disinformation) and mitigation measures mentioned therein. There have been mentions of the creation of rapid-response systems to exchange information with CSOs, fact-checkers, other platforms and authorities specifically in the content of disinformation and misinformation and elections. As stated in the Commission Opinion on the assessment of the Code of Practice on Disinformation: *"the Code of Practice on Disinformation can serve as a significant and meaningful benchmark of DSA compliance for the providers of VLOPs and VLOSEs that adhere to and comply with its Commitments"*[26]. In particular, the value of the Code lies in the fact that is a comprehensive set of commitments and measures voluntarily agreed by a wide range of the stakeholders (e.g. VLOPs and VLOSEs providers, CSOs, advertising industry), identifying best industry practices to mitigate risks linked to the spread of disinformation. Therefore, the Code constitutes an important source of mitigation measures.

4.9. Awareness-raising

Article 35(1)(i) DSA refers to the following mitigation measures for providers to put in place: *"taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information"*.

In order to improve awareness and give users more information about systemic risks, providers mentioned the creation of knowledge or information panels for authoritative information about elections or crises events, the creation of media literacy campaigns, the creation of wellness help pages for users and creators (e.g. for bullying and harassment mental well-being resources), privacy and safety pages, user helplines and guides to the attention of parents and guardians. Other measures such as the displaying of banners with information for users and creators to consider before commenting or uploading content, labels informing that an account has been verified or that content has been fact-checked have also been mentioned by providers. Some CSOs suggested awareness raising measures about the systemic risks of excessive social media usage, especially for minors and first-time users or after the introduction of new features.

[26] Commission Opinion of 13 February 2025 on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 of Regulation 2022/2065, C(2025) 1008 final, available at the following link: https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.

5. Outlook

This is the first edition of the yearly report referred to in Article 35(2) DSA. The accumulation of future editions will, over time, provide a long-term perspective on which systemic risks are the most prominent and recurrent from year to year. It will also build on the enforcement measures taken with regard to providers. The DSA, including Articles 34 and 35, is still at an early stage of its implementation. Future editions will also benefit from the developing expertise of stakeholders, including researchers and representatives of CSOs. Developments in the implementation and enforcement of other DSA provisions such as the data access mechanisms of Article 40, and notably the research outputs resulting from such data access, will contribute to the wealth of information that will feed into an ever better understanding of systemic risks as well as mitigation measures under Articles 34 and 35 DSA.

Annex: Resources and studies from independent experts and civil society organisations

The lists below contain public resources and studies from independent experts and CSOs as well as input from CSOs, trusted flaggers and Member State authorities collected by the Board and the Commission either upon invitation or through spontaneous submissions.

List of independent experts and CSOs that submitted input for this report to the Board and the Commission in April 2025:

- 5rights
- 7amleh
- A Jewish Contribution to an Inclusive Europe (CEJI)
- Addiction France
- Agence France Presse (AFP)
- AlgorithmWatch
- Alliance4Europe
- Austrian Fund for the Documentation of Religiously Motivated Political Extremism
- BodyWhys
- Center For Digital Paedagogik (CFDP)
- Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)
- Civil Liberties Union for Europe (Liberties)
- Comunicare
- Conseil Représentatif des Institutions Juives de France (Crif)
- Deutsches Kinderhilfswerk (DKHW)
- Digitale Chancen
- Digitalt Ansvar
- E-enfance
- EU Disinfo Lab
- Eurochild
- European Fact-Checking Standards Network (EFCSN)
- European Partnership for Democracy (EPD)
- Foundation Diaspora in Action for Human Rights and Democracy (formerly Foundation The London Story)
- Freepressunlimited
- Fundación Maldita
- Fundación Secretariado Gitano
- Global Witness
- HateAid
- In IUSTITIA
- Integrity Institute
- International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA)

- International Network Against Cyber Hate (INACH)
- Knight-Georgetown Institute
- Medierådet for Børn og Unges
- Österreichisches Institut für angewandte Telekommunikation (OIAT)
- Panoptykon Foundation
- Pointdecontact
- Rathenau
- Red Barnet (Save the Children Denmark)
- Reporter Sans Frontières
- Reset Tech
- Savati Copiii (Save the Children Romania)
- Social Media Exchange (SMEX)
- SOS Racisme
- The Foreign Policy Centre
- Verbraucherzentrale Bundesverband
- WhatToFix

List of other sources from independent researchers and CSOs which were considered for input for this report of the Board and the Commission (in reverse chronological order):

Author / organisation	English title	Date	Link
Open Evidence, PPMI, Spark Legal	DSA study on systemic risks and their mitigation (EC-CNECT/2024/OP/0032) *(study commissioned by the Commission inter alia for the purpose of supporting this report and that is not intended for a self-standing publication)*	July 25	n/a
Marie-Therese Sekwenz, Rita Gsenger, Scott Dahlgren, Ben Wagner	Doing Audits Right? The Role of Sampling and Legal Content Analysis in Systemic Risk Assessments and Independent Audits in the Digital Services Act	May 2025	Link
Science Feedback, Who Targets Me	Online misinformation pays. Why? Taking stock of a broad range of evidence	April 2025	Link
Stanford University	Stanford Youth Safety and Digital Wellbeing Report, 2025	April 2025	Link
Gianclaudio Malgieri, Cristiana Santos	Assessing the (severity of) impacts on fundamental rights	April 2025	Link
Deloitte, Zentrum für Psychosoziale Medizin des Universitätsklinikums Hamburg-Eppendorf (UKE)	Societal impacts of digital services with a view to addiction risks *(study commissioned by the German DSC)*	March 2025	Link

Knight-Georgetown Institute, Panoptykon Foundation	Better Feeds: Algorithms That Put People First	March 2025	Link
Civil Liberties Union for Europe, European Partnership for Democracy	Beyond Disinformation: How DSA Risk Assessments Ignore Democracy's Real Threats	March 2025	Link
DSA Civil Society Coordination Group	Initial Analysis on the first round of risk assessment reports under the EU Digital Services Act	March 2025	Link
Civil Liberties Union for Europe, European Partnership for Democracy	Civic Discourse and Electoral Processes in the Risk Assessment and Mitigation Measures Reports under the Digital Services Act	March 2025	Link
Alexander von Humboldt Institut für Internet und Gesellschaft	"Societal impact of systemic risks" *(study commissioned by the German DSC)*	March 2025	Link
Global Counsel	Online safety: the next wave of regulation	March 2025	Link
Centro de Estudios en Libertad de Expresión y Acceso a la Información	Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation	March 2025	Link
Mateus Correia de Carvalho	It will be what we want it to be: Socitechnical and contested systemic risk at the core of the EU's regulation of platforms' AI systems	March 2025	Link
Ahnul Ha, Yun Jeong Lee, Marvin Lee, *et al.*	Digital Screen Time and Myopia: A systematic review and dose-response meta-analysis	February 2025	Link
Integrity Institute	Global Transparency Audit	February 2025	Link
Integrity Institute	Risk assessment guidance and initial analysis	February 2025	Link
Integrity Institute	Risk dimensions and mitigation effectiveness	February 2025	Link
David Sullivan	Systemic Risk Assessments Hold Clues for EU Platform Enforcement	February 2025	Link
Amnesty International	Meta's new content policies risk fuelling more mass violence and genocide	February 2025	Link
Center for Democracy and Technology	EU Tech Policy Brief: January 2025	February 2025	Link
Electronic Frontier Foundation	Systemic Risk Reporting: A System in Crisis?	January 2025	Link

Knight-Georgetown Institute	Advancing Platform accountability: The promise and perils of the DSA RAs	January 2025	Link
Institute for Strategic Dialogue	"Identification, assessment and management of systemic risks in the context of the Digital Services Act" *(study commissioned by the German DSC)*	January 2025	Link
Tim Bernard	Reading the Systemic Risk Assessments for Major Speech Platforms: Notes and Observations	December 2024	Link
Merve Sambel Aykutlu, Hasan Cem Aykutlu *et al.*	Digital media use and its effects on digital eye strain and sleep quality in adolescents: a new emerging epidemic?	December 2024	Link
Mark Scott	5 Things to Know about the Digital Services Act's First Risk Assessments and Audits	December 2024	Link
DSA Observatory	DSA risk assessment reports: a guide to the first rollout and what's next	December 2024	Link
Centre on Regulation in Europe (CERRE)	Evaluating systemic risk management under the DSA	December 2024	Link
Sally Broughton Micova, Bryn Enstone	What to Do with the Long-Awaited DSA Systemic Risk Assessments	November 2024	Link
Center for Democracy and Technology *et al.*	Joint Civil Society Statement on Meaningful Transparency of Risk Assessments under the Digital Services Act	November 2024	Link
AlgorithmWatch	Researching Systemic Risks under the Digital Services Act	July 2024	Link
Centre on Regulation in Europe (CERRE)	Cross-Cutting issues for DSA systemic risk management: an agenda for cooperation	July 2024	Link
Institute for Strategic Dialogue	Identifying sock-puppets on Wikipedia: a semantic clustering approach	April 2024	Link
Crossover.social	"Up next", biased politics? YouTube recommendations and political bias in the Finnish Presidential elections 2024	March 2024	Link
Electronic Frontier Foundation, Article 19	Disinformation and Elections: EFF and ARTICLE 19 Submit Key Recommendations to EU Commission	March 2024	Link
Panoptykon Foundation	Joint-Submission on the Commission's Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes	March 2024	Link
Panoptykon Foundation	Safe by default: Moving away from engagement-based rankings towards safe, rights-respecting, and human centric recommender systems	March 2024	Link
AlgorithmWatch	Ensuring legitimacy in stakeholder engagement: the '5 Es' framework	February 2024	Link

Civil Liberties Union for Europe, European Partnership for Democracy	Identifying, analysing, assessing and mitigating potential negative effects on civic discourse and electoral processes: a minimum menu of risks very large online platforms should take heed of	January 2024	Link
Verbraucherzentrale Bundesverband	100 days of the Digital Services Act: consumer protection on online platforms still insufficient	December 2023	Link
AI Forensics	An analysis of Microsoft's copilot in Swiss and Bavarian elections	November 2023	Link
AI Forensics, Amnesty International	TikTok's role in youth mental health	November 2023	Link, link
Joan Barata, Jordi Calvet-Bademunt	The European Commission's Approach to DSA Systemic Risk is Concerning for Freedom of Expression	October 2023	Link
AI Forensics	Amazon's risky recommendations	October 2023	Link
Access Now, European Center for Not-for-Profit Law	Towards meaningful fundamental rights impact assessments under the DSA	September 2023	Link
Irish Council for Civil Liberties, Panoptykon Foundation, People vs BigTech and al.	Fixing Recommender Systems	August 2023	Link
AlgorithmWatch	Making sense of the DSA: How to define platforms' systemic risks to democracy	August 2023	Link
David Sullivan, Jason Pielemeier	Unpacking "Systemic Risk" Under the EU's Digital Service Act	July 2023	Link
Centre on Regulation in Europe (CERRE)	Elements for effective systemic risk assessment under the DSA	July 2023	Link
Alessandro Mantelero	Fundamental rights impact assessments in the DSA	November 2022	Link
Amnesty International	What the EU's Digital Services Act means for human rights and harmful Big Tech business models	February 2022	Link