EUROPEAN BOARD FOR DIGITAL SERVICES

Second 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 risk as well as mitigation measures

1 July 2026

EUROPEAN BOARD FOR DIGITAL SERVICES

Table of contents

Chapter 1

What this report is about and how it is structured

1. What this report is about and how it is structured

1.1. Background to this report

The Digital Services Act ("DSA") sets out rules for regulating online intermediary services, from online marketplaces[1] (including app stores), social networks, to pornographic content platforms and online search engines. Enforcement and supervision of the rules is shared by the European Commission and Digital Services Coordinators ("DSCs") who coordinate and work together in the European Board for Digital Services ("the Board").

The DSA includes a risk management framework (Articles 34 and 35) applicable to online platforms with the widest reach and therefore the most potential for impact on the recipient of their services: Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), defined as services with at least 45 million monthly active recipients in the Union, or 10% of the Union's population.

Article 34(1) DSA requires providers of VLOPs and VLOSEs to identify, analyse and assess any systemic risks arising from how their services are designed, how they function and how they are used in practice, including their algorithmic systems. Article 35(1) DSA requires that providers of VLOPs and VLOSEs put in place reasonable, proportionate and effective mitigation measures tailored to the specific systemic risks identified in their risk assessments. In doing so, providers must have particular consideration for the impacts of such measures on fundamental rights, including the right to freedom of expression. The obligation to conduct risk assessment reports to identify, assess and mitigate systemic risks takes place annually. VLOPs and VLOSEs must transmit the reports concerning their risk assessments (including the ad hoc risk assessment reports prior to deploying new functionalities), the risk mitigation measures that they have implemented, as well as the compliance audits to their Digital Services Coordinator of establishment and to the Commission. In accordance with Article 42 DSA providers must, upon completion, publish all those reports without undue delay . This also includes ad hoc risk assessment reports (i.e. assessments performed prior to deploying new functionalities that are likely to have an impact on the risks) transmitted to the Commission and the DSC of establishment in that yearly cycle. These provisions apply exclusively to VLOPs and VLOSEs. Other intermediary services are not subject to the risk management framework of Articles 34 and 35 DSA.

Recital 90 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*

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

of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations".

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 report is the second year's edition of the Article 35(2) report. The first edition was adopted by the Board and published on 18 November 2025[2].

The aim of this Article 35(2) report is to provide 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 third-party stakeholders, such as academics, independent researchers, civil society organisations ("CSOs"), trusted flaggers and Out-of-Court Dispute Settlement Bodies ("ODSBs"), and an overview of certain risk mitigation practices. With regard to risk mitigation, this second edition, like the first one, focuses on reported practices without singling out any as "best" or "good" practice. Over time, and in light of accumulating experience with DSA implementation and enforcement in practice, future editions of this report will also aim to identify evolving best practices for the mitigation of systemic risks.

Chapter 3 on systemic risks is structured according to the order in which risks are mentioned in Article 34(1) DSA. Some risks are grouped together to improve readability . Chapter 4 on risk mitigation measures is based on Article 35(1) DSA but, contrary to last year's report, goes beyond solely mirroring the structure of the article. Namely, it also distinguishes between different types of intermediary services. Two designated services, Google Maps and Wikipedia, do not fall within the categories chosen but mitigation measures that may be relevant for them are still included.

[2] 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, available at the following link: https://digital-strategy.ec.europa.eu/en/news/press-statement-european-board-digital-services-following-its-16th-meeting.

1.2. The DSA risk management framework as a key safeguard for the protection of minors

One of the aims of the DSA according to its Article 1 is to set out "*harmonised rules for a safe, predictable and trusted online environment*", including for minors.

The protection of minors online is a key priority in the Union. According to a 2025 Eurobarometer survey[3] *over 9 in 10 Europeans* were in favour of action to protect minors against *"the negative impact of social media on their mental health (93%), cyberbullying and online harassment (92%) and assuring mechanisms to restrict age-inappropriate content (92%)".*

It therefore does not come as a surprise that the first working priority for the Board in its Q4/2025 to Q4/2026 Annual Work Plan is *"Boosting online safety for minors across the European Union"*[4].

During the reporting period, Members of the Board observed risks to the protection of minors on VLOPs and VLOSEs throughout the Union. Members of the Board highlight for example risks related to compulsive or addiction-like behaviour on social media, risks related to the exposure to harmful content including dangerous social media challenges, and harmful behaviour such as cyberbullying and grooming. Members of the Board also stress risks related to children's access and exposure to adult content.

Members of the Board are closely monitoring and supporting the Commission in identifying systemic risks across the Union, to detect emerging patterns and trends.

This report is therefore also an occasion to highlight that the risk management framework - as a cornerstone of the DSA - is a tool to support the protection of minors online. In addition to obligations under Article 28 DSA, the DSA's risk management framework is essential to ensure that enforcement of the DSA concerning the protection of minors keeps pace with technological developments. It enables the flexible identification of features that may be harmful to minors, and supports actions that consider children's specific vulnerabilities when using VLOPs and VLOSEs. That being said, the Board would like to emphasise the importance of mitigating risks to the protection of minors online for the broader benefit of all users. Indeed, while minors are a particularly vulnerable group online, any individual may be exposed when using VLOPs and VLOSEs to content or design features which may, for example, lead to negative consequences for their health and well-being, whether they are minors or not. Therefore, mitigation measures implemented to prevent harmful features or activities online may not only be relevant to

[3] Special Eurobarometer 566 - The State of the Digital Decade Eurobarometer report February-March 2025, available at the following link: https://europa.eu/eurobarometer/surveys/detail/3362.
[4] European Board for Digital Services, Annual Work Plan Q4/2025 to W4/2026, available at the following link: https://ec.europa.eu/newsroom/dae/redirection/document/121774.

protect minors, but can further benefit all users by contributing to an overall safer online environment.

The Board and the Commission recall that:

- Article 34(1)(b) DSA requires providers of VLOPs and VLOSEs to diligently identify, analyse, and assess any actual or foreseeable negative effects on the exercise of the rights of the child enshrined in Article 24 of the Charter of Fundamental Rights;
- Article 34(1)(d) DSA requires providers of VLOPs and VLOSEs to diligently identify, analyse, and assess any actual or foreseeable negative effects in relation to the protection of minors;
- Article 35(1)(j) DSA requires providers of VLOPs and VLOSEs to put in place reasonable, proportionate, and effective *"targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate".*

During the preparation of this report, the Board and the Commission found that providers and CSOs observed systemic risks in relation to the protection of minors on VLOPs and VLOSEs stemming from the design and functioning of their services and their related systems as well as from the use made of their services. Indeed, systemic risks in relation to the protection of minors are amongst the most prominent and recurrent. These include, for example, grooming, the exposure to harmful content, unsafe account settings and addictive designs. Importantly, risks to the protection of minors intersect with other systemic risks. For example, they intersect with risks related to the fundamental rights to private and family life and data protection (e.g. in the context of cyberbullying, stalking or doxxing) or consumer protection (e.g. in the context of scams). Such intersections are presented in further detail in Chapter 3 of this report.

Systemic risks may be mitigated or aggravated by several factors. For example, business models aimed at maximising user engagement and time spent on a service may lead providers of VLOPs and VLOSEs to make design choices that may aggravate systemic risks, including in relation to the protection of minors. Relevant risk factors in this regard include, amongst others:

- ***Artificial intelligence (AI) systems:*** Generative AI features embedded in VLOPs and VLOSEs may be used in ways which can be harmful to minors. Likewise, the dissemination of AI-generated content on VLOPs and VLOSEs may increase risks related to the protection of minors online. For example, AI-generated sexual deepfakes, predominantly of women and minors, have been widely disseminated on some VLOPs and VLOSEs. Concerns have also arisen in relation to the use of AI chatbots and their potential impacts on the mental well-being of minors as well as on the dissemination of illegal content such as Child Sexual Abuse Material (CSAM).
- ***Recommender Systems:*** Recommender systems designed to maximise engagement and time spent on a platform may lead to well-being risks linked to compulsive or addiction-

like use, as well as risks linked to the amplification of content that could have a negative impact on minors' mental health and wellbeing.

This report presents some measures taken by providers of VLOPs and VLOSEs to mitigate systemic risks in relation to the protection of minors online. However, the measures presented in this report should not be interpreted as "best", or even "good" practices. For now, the report only attempts to map and organise the range of mitigation approaches currently observed across different providers. Such measures include, for example, age restriction policies, the detection and removal of CSAM through hash and match methods, or the use of protective default settings for minors such as disabling infinite scrolling and autoplay features by default, content blurring, warning labels, and trigger warnings for graphic content. These measures are presented in detail in Chapter 4 of this report.

Beyond the risk management framework, the DSA also contains a comprehensive set of safeguards to protect minors online in the Union:

- ***Specific rules dedicated to the protection of minors online:*** Article 28 DSA requires providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors on their services. This includes, under Article 28(2) DSA, that providers of online platform shall not present advertisements on their interface based on profiling, using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. Furthermore, on 14 July 2025, the Commission adopted Guidelines under Article 28 DSA. According to their paragraph 3: *"These guidelines aim to support providers of online platforms in addressing* [risks to the protection of minors] *by providing a set of measures that the Commission considers will help these providers to ensure a high level of privacy, safety and security of minors on their platforms, which will contribute to the protection of minors, which is an important policy objective of the Union"*. The Commission is utilising these Guidelines as a benchmark for the supervision and enforcement of compliance with Article 28 DSA.

- ***Easily understandable terms and conditions:*** Article 14 DSA stipulates that where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.

- ***Online advertising transparency:*** Article 39 DSA requires providers to make publicly available a repository of advertisements and the information they contain. Recital 95 DSA adds that repositories should include information about *"targeting criteria and delivery criteria, in particular when advertisements are delivered to persons in vulnerable situations, such as minors".*

- *TRANSPARENCY DATABASE:* The DSA Transparency Database contains a filter in its dashboard to track statements of reasons under Article 17 DSA for content moderation decisions related to the protection of minors.
- *DEVELOPMENT OF STANDARDS:* Under Article 44(1)(j) DSA, the Commission shall consult the Board, and shall support and promote the development and implementation of voluntary standards set for targeted measures to protect minors online.

Lastly, the Board and the Commission would like to thank the CSOs that provided input to this report. Contributions by CSOs and independent researchers continue to inform the preparation of the Article 35(2) reports and help support the monitoring of systemic risks in the Union.

1.3. Reporting period and relationship with DSA enforcement activities

This report covers the reporting period between 17 February 2025 and 16 February 2026. This reporting period starts the day after the end of the reporting period for last year's Article 35(2) report and lasts for one year from then on.

Nothing in this report should be interpreted as guidance for the compliance with Articles 34 and 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.

Chapter 2

How this report was prepared

2. How this report was prepared

To prepare this report, the Board consulted a diverse range of sources highlighted below.

- The published versions[5] of the risk assessment reports that providers of the 23 VLOPs[6] and 2 VLOSEs[7] transmitted between 17 February 2025 and 16 February 2026 to the Commission and their DSC of establishment[8];
- The published versions of Article 37 DSA audit reports prepared by independent audit organisations and transmitted between 17 February 2025 and 16 February 2026 to the Commission and their DSC of establishment;
- Other DSA transparency outputs prepared by VLOPs and VLOSEs providers:
    - Article 39 DSA advertisement repositories, which allow users and other stakeholders including CSOs, researchers and public institutions to better understand whether and how advertising systems influence any of the systemic risks under Article 34(1) DSA, for example by searching and querying the repositories for details about advertisements including information about who paid for the advertisement, targeting parameters and total number of users reached;
    - 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;
    - Articles 15, 24 and 42(2) DSA transparency reports made available to the public by VLOPs and VLOSEs providers on content moderation;
    - The Article 25(4) DSA Transparency Database[9] that makes all Article 17 DSA statements of reasons available to the public. The DSA requires VLOPs 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

[5] The 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.

[6] Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Stripchat, Temu, TikTok, Twitter (now X), Wikipedia, YouTube, XNXX, XVideos, Zalando.

[7] Bing, Google Search.

[8] The Commission published a Q&A on risk assessment reports, audit reports and audit implementation reports under Article 42 DSA in November 2024 (and updated in February 2026) in order to provide more information about the reporting and publication obligations, *"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.

[9] DSA Transparency Database, available at the following link: https://transparency.dsa.ec.europa.eu/.

and facilitates scrutiny over content moderation decisions as it allows to track the content moderation decisions taken by providers of online platforms in almost real time.

- Biannual reports[10] of the VLOPs and VLOSEs signatories of the Code of Conduct on Disinformation, which has been integrated into the framework of the DSA pursuant to Article 45 DSA as of 1 July 2025.
- Input gathered through studies contracted by the Commission as well as by DSCs (these studies are listed 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;
- Input from CSOs, trusted flaggers under Article 22 DSA[11] and Out-of-Court Dispute Settlement Bodies under Article 21 DSA.
- Input from 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 current scientific insights to identify the analyses and observations most relevant and robust for inclusion in this report. This approach reflects the evolving nature of the evidence base. Future iterations of the yearly Article 35(2) DSA reports are expected to build on an even stronger scientific foundation, as additional insights emerge, for instance from data accessed through Article 40 DSA data access mechanism. This report focuses on systemic risks and mitigation measures reported on by the VLOPs and VLOSEs providers. At the same time, it also takes into account systemic risks and mitigation measures not identified by VLOPs and VLOSEs providers but corroborated by several independent experts from research institutions and CSOs, helping to provide a complete and more balanced picture.

[10] The bi-annual reports are available at the following link: https://disinfocode.eu/reports.

[11] According to Article 22 DSA, trusted flagger status is awarded by DSCs to an applicant that meets all of the following conditions: it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content, it is independent from any provider of online platforms, it carries out its activities for the purposes of submitting notices diligently, accurately and objectively.

Chapter 3

The most prominent and recurrent systemic risks identified

3. The most prominent and recurrent systemic risks identified

This Chapter presents an overview of the most prominent and recurrent systemic risks as reported by providers of VLOPs and VLOSEs, or as identified through other information sources. Such risks may materialise in different ways and to varying degrees across services, depending, inter alia, on the nature of the services and their use. For example, the most prominent systemic risks identified on online marketplaces are likely to differ from those arising on search engines. Additionally, systemic risks related to illegal content or civic discourse may manifest differently across Member States, for instance due to regional and linguistic specificities and differing definitions of illegal content. In contrast, other risks, such as those linked to interface design, are more likely to be present in a relatively uniform manner 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. Beyond the identification of systemic risks, this Chapter also illustrates how certain risk factors referred to in Article 34(2) DSA may influence those risks. These factors should be considered both individually and in combination with each other, as their interaction may shape the emergence and impact of systemic risks.

The fact that a systemic risk is described as recurrent does not imply that it remains static over time. As highlighted in Article 35 DSA, developments at Member State level may also be relevant. Such developments, alongside technological and societal changes, influence how risks arise and evolve, making it necessary to continuously update the evidence base and understanding of systemic risks. In this context, recital 90 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".

The DSA further introduced mechanisms that support the ongoing scrutiny of systemic risks. In addition to the obligation for providers of VLOPs and VLOSEs to conduct risk assessments at least once a year and prior to the deployment of functionalities likely to have a critical impact on identified risks, this includes independent compliance audits under Article 37 DSA, audit implementation reports, transparency reporting on content moderation under Articles 15 and 42 DSA, and the data access framework set out in Article 40 DSA.

The following sections include text boxes with examples of systemic risks and risk factors. These are included for illustrative purposes only, to show how such risks have been described by providers or CSOs. They do not constitute an evaluation of any provider's approach, nor does the selection or ordering of examples imply any ranking of importance. Likewise, the examples relating to risk factors are not intended to provide a comprehensive overview of all risk factors observed. Unless stated otherwise, text drafted outside of text boxes relates to systemic risks from interface design or organic content, while systemic risks related to advertising are described in the risk factor text boxes. Moreover, throughout this Chapter (and the remainder of the report), certain paragraphs open with ***IN-LINE TITLES IN BOLD AND ITALICS*** which are intended to group systemic risks or mitigation measures into sub-categories for readability purposes.

3.1. Illegal content

A central objective of the DSA is to contribute to combatting the dissemination of illegal content. This aim is affirmed in Article 1 DSA and across several recitals, including recital 12, which underscores the importance of *"a safe, predictable and trustworthy online environment"*. The DSA does not define what constitutes "illegal content" but, amongst other things, focuses on how systems, processes, designs, practices and policies may contribute to the dissemination of illegal content and to other systemic risks. The determination of what is illegal is left to Member State law, or other provisions of Union law. Under Article 3(h) DSA, *"'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"*.

Risk assessment obligations under the DSA further reflect this focus. Article 34(1)(a) DSA requires providers of designated VLOPs and VLOSEs to include in their risk assessments the systemic risks related to *"the dissemination of illegal content through their services"*. Recital 80 illustrates the types of illegal content 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 form part of a broader enforcement system on illegal content: the DSA provisions on notice and action mechanisms (Article 16), trusted flaggers (Article 22), and orders to act against illegal content (Article 9) are all central to this framework. Beyond the DSA itself, systemic risks linked to illegal content are also addressed through other pieces of Union legislation, such as the Terrorist Content Online Regulation ("TCO")[12].

Crucially, any actions taken by providers of VLOPs and VLOSEs under the DSA to combat the dissemination of illegal content must be aligned with fundamental rights, including the right to freedom of expression and information, which lies at the heart of the DSA. It is to that end that the DSA requires all online platforms to be transparent and to enable scrutiny of their moderation decisions, including by informing users of those decisions and permitting them to appeal[13], internally and through Out-of-Court Dispute Settlement Bodies, or directly to Member States' courts. More broadly, the DSA establishes clear rules on transparency, accountability and empowerment.

Risks related to the dissemination of illegal content have been identified by all VLOPs and VLOSEs providers in their risk assessment reports. The section that follows outlines the most prominent and recurrent systemic risks identified in this context.

3.1.1. Illegal products, services and activities

Risks related to the dissemination of illegal, unsafe or restricted products were identified by nearly all providers and CSOs, but in particular with regard to online marketplaces and social media. The dissemination of content related to illegal or restricted services, as well as the conduct of illegal activities, were also reported by nearly all providers and CSOs. The dissemination of illegal content may have impacts on other systemic risks. For example, some illegal products such as weapons may pose a threat to public health or security, while the dissemination of illegal or restricted services may have a negative effect across a range of rights

[12] 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.

[13] The DSA Transparency Database contains extensive data on e.g. VLOPs content moderation decisions which have been reversed thanks to appeals.

and areas, including gender-based violence, the protection of minors, and consumer protection.

- *THE DISSEMINATION OF ILLEGAL PRODUCTS.* Examples of illegal products identified by providers and CSOs included, for example, unsafe, dangerous and/or non-compliant products (e.g. lacking CE markings, or products including toys made with hazardous or prohibited materials or substances), live animals (including endangered animal species), illegal drugs (including psychoactive substances), alcohol, tobacco and other regulated substances, medical products and devices which may only be marketed via regulated channels (e.g. prescription drugs), weapons, ammunition and explosives (including precursors), hazardous chemicals and pesticides, unsafe electrical goods, and IP-infringing products such as counterfeits. The dissemination of fake ID cards, passports, licenses, and other government-issued documents has also been identified by Members of the Board.
- *ILLEGAL SERVICES AND THE CONDUCT OF ILLEGAL ACTIVITIES.* Providers and CSOs reported systemic risks related to the provision of illegal services and activities such as:
  - drug trafficking, and traffics of other illegal or dangerous substances;
  - trafficking in human beings and illegal migrant smuggling;
  - money laundering and terrorism financing;
  - sales and exchanges of high amounts of cash currency;
  - violent activities (e.g. sextortion, hiring to harm, kill, harass, doxx, kidnap, stalk);
  - illegal sexual services, including illegal prostitution;
  - non-consensual sharing of intimate images and recordings;
  - (financial) scams and fraud;
  - illegal gambling;
  - illegal offers of accommodation;
  - violation and fraud of the rules governing distance selling and provision of online services (e.g. through deepfakes and digitally created Value Added Tax (VAT), altered photorealistic video or audio);
  - violation of Protected Designations of Origin (e.g. for agricultural products).

Examples of **risk factors** concerning systemic risks related to **illegal products, services and activities**:

Content moderation systems: The reappearance of products and related sellers, who, for example, may make superficial changes to product attributes or attempt to reappear under the same or different identities has been noted by providers as a content moderation challenge for illegal goods. Furthermore, there is a risk that ratings or reviews are misused to facilitate or promote the sale of illegal goods. On social media, malicious actors may also

covertly exchange restricted goods, using emojis, slang and signposting to harmful external sites, or by posting branded content as organic without labelling.

Monetisation policies and their enforcement: Some CSOs noted that platforms' monetisation policies may aggravate the dissemination of illegal content, and lead, for example, to indirectly financing illegal activities including from criminal organisations.

Intentional manipulation of the services and AI systems: Providers of online marketplaces have reported fake or manipulated reviews, with generative AI enabling malicious actors to produce realistic fake reviews at scale. Some CSOs observed that the increasing integration of AI tools into VLOPs and VLOSEs may lead to financial extortion or coercion. Some CSOs highlighted the trend of AI-manipulated photos making individuals appear unclothed, and thereby potentially producing child sexual exploitation material which may then be disseminated on VLOPs and VLOSEs.

Specific regional or linguistic aspects: Providers of online marketplaces have emphasised that the scale and multilingual nature of product listings and user bases heighten the risk of missing disclosures, potentially misleading consumers and complicating consistent oversight. Providers also mentioned the use of slang to circumvent content moderation systems, for example to dissimulate the sale of illegal drugs on social media.

Examples of observations by providers and CSOs concerning systemic risks related to illegal products, services and activities:

Booking, 2025 DSA risk assessment report, p. 29: *"We recognize there is a risk that ill-intended users may seek to use the Booking.com platform to promote illegal products and services (e.g. related to drugs, gambling, underage drinking), or offer illegal or unlicensed (accommodation) services, which directly contravenes our policies and applicable laws"*.

Apple App Store, in its 2025 DSA risk assessment report at p. 10 mentioned a "*risk that an app store could be used to disseminate certain categories of illegal content to users in the EU, including: 1. apps designed to disseminate illegal content or facilitate illegal behaviours, such as fraud, including "bait-and-switch" apps, or apps that are designed to undermine fundamental rights; 2. apps that infringe the intellectual property rights of others; and 3. apps that facilitate activities that are illegal in certain Member States (for example, certain types of real money gambling)*".

Temu, 2025 DSA risk assessment report, p. 31: *"Lack of compliance awareness among non-EU traders: While Temu's cross-border and diverse trader community enhances product variety, it also contributes to the likelihood that certain third-party traders, in particular those*

based outside of the EU, may lack sufficient knowledge of applicable EU legislation governing product safety, IP protection, and digital commerce or the recent legislative updates or amendments. […] *Without sufficient awareness training, certain traders may inadvertently list non-compliant products on EU country sites"*.

3.1.2. Sexual abuse material, including Child Sexual Abuse Material ("CSAM")

VLOPs and VLOSEs providers, in particular pornographic platforms and social media, have identified systemic risks related to adult sexual abuse and child sexual abuse material (CSAM). These systemic risks are related to others, such as risks to the rights to private and family life and personal data protection, gender-based violence (GBV), the protection of minors, as well as illegal activities such as human trafficking, particularly where sexual exploitation occurs for profit.

CSAM. Providers and CSOs identified risks related to CSAM content, including the coercion and solicitation of minors for the production of self-generated CSAM, as well as borderline CSAM content (e.g. content that sexualises minors, glorifies or legitimises child abuse). Relatedly, some CSOs observed risks that children experience the sharing of intimate images, including screenshots or videos, about them being shared to others, including (unknown) adults, against their will. Some CSOs also mentioned risks of children receiving sexual material from adults.

ADULT SEXUAL ABUSE. Systemic risks of adult sexual abuse content have been identified by providers and CSOs as prominent and recurrent. This can relate for example to abuses in the context of illegal activities such as illegal prostitution or trafficking in human beings, but also to risks of influencers on social media and performers on pornographic platforms being abused or stalked by other users or creators. Trafficking in human beings risks are also closely linked to GBV, as women and girls are disproportionately affected, particularly in cases of sexual exploitation. Other marginalised groups — including migrants, LGBTQ+ individuals, and economically vulnerable populations — may also face elevated risks of trafficking. Within their risk assessments, some platform providers recognise that their services may be misused to facilitate trafficking-related activities, including the coordination or advertisement of exploitative services. The risk of trafficking in human beings for sexual exploitation is specifically mentioned in pornographic platforms' risk assessments.

Examples of **risk factors** concerning systemic risks related to **sexual abuse content**:

Design and platform features: Platform design and functionalities may influence the likelihood of CSAM and related risks manifesting. Features such as direct messaging have been mentioned by some providers as facilitating private interactions, and thus lead sexual offenders to contact minors, facilitate grooming, or solicit and distribute CSAM. Private

messaging functions may also be used to redirect users off-platform to websites displaying CSAM.

AI systems: Generative AI has been mentioned by some providers and CSOs as a risk factor in relation to CSAM risks, as it may be misused to facilitate abusive behaviour, including by providing guidance that supports grooming or sextortion of minors, and generating synthetic or manipulated CSAM (e.g. non-identifiable and artificially generated depictions of minors).

Intentional manipulations of the services: Coordinated inauthentic behaviour has been outlined as an additional risk factor by some social media providers and CSOs, as it may drive engagement and expand distribution networks of CSAM.

Monetisation policies and their enforcement: Additionally, researchers observed accounts which have been disseminating content that sexualises minors, including both authentic and artificially generated material, and in some cases leveraging platform features to monetise such activity or redirect users to external services. These accounts often display coordinated or automated patterns of behaviour, including the systematic use of hashtags, amplification strategies, and cross-platform linking. According to some CSOs, subscription and tipping features may be misused to commercialise content sexualising minors, with platforms retaining a share of the resulting revenue.

Examples of observations by providers and CSOs concerning systemic risks related to sexual abuse content:

Facebook, 2025 DSA risk assessment report, p. 71: *"We observe behaviour such as intentional manipulation by threat actors to persistently adapt to evade detection, use of implicit signals like keywords and hashtags (e.g., "chicken soup"), moving conversations off the service (e.g., via posting links to off-platform sites) to take advantage of minors and/or spread violating content (e.g., CSAM), and returning to the service through new accounts despite being blocked"*.

TikTok, 2025 DSA risk assessment report, p. 37: *"TikTok considers that the dissemination of CSAM content may involve users attempting to use the Platform to: Share, re-share or offer to trade or sell, or direct users of the Platform to obtain or distribute CSAM content; Generate and/or share CSAM, including self-generated CSAM; Disseminate content that depicts, solicits, glorifies or encourages child abuse imagery including nudity, sexualised minors or sexual activity with minors; or Disseminate content that depicts, promotes, normalises or glorifies paedophilia or the sexual assault of a minor"*.

Stiftung Digitale Chancen, a CSO specialised on digital rights, submission to the invitation for contributions from the European Board for Digital Services and the European Commission:

"The amount of child sexual abuse imagery, deep fake nudes and sexualized violence against women on platforms is increasing rapidly via AI tools and functionalities being embedded in social media platforms".

Pornhub, in its 2025 DSA risk assessment report mentioned risks such as *"Child sexual abuse Material"* (p. 8), *"AI generated content representing illegal acts"* (p. 36), *"Sex trafficking"* (p. 41) as well as *"Pornography fostering abuse and violence"* (p. 67).

Google, 2025 DSA risk assessment report, at p. 32, mentioned the risk of: *"The use of generative AI to support other child sexual abuse behaviours, such as providing text instructions on how to carry out abuse, supporting offenders to groom or sextort minors, or promoting or normalising sexual interest in minors"*.

3.1.3. Content from terrorist groups, violent groups and sanctioned entities

Providers of VLOPs and VLOSEs such as social media and search engines as well as CSOs have noted in particular risks related to terrorist groups, violent groups and sanctioned entities. Such risks are also relevant to other areas, such as civil discourse, electoral processes and public security as well as, in certain cases, the protection of minors. While the dissemination of such content may fall under legal exemptions in certain contexts (e.g. dissemination for educational, journalistic, artistic or research purposes or to raise awareness), systemic risks may arise where platforms are misused by terrorist groups and their sympathisers to disseminate terrorist content online in order to spread their message, to radicalise and recruit followers, and to facilitate and direct terrorist activity. Such risks encompass, for example, the dissemination of terrorist imagery and propaganda (e.g. symbols, slogans, gestures in contexts other than e.g. journalism), the praise, glorification of terrorism, terrorism financing, radicalising, recruiting and training terrorists (including minors, and including with the aim of using individuals as "disposable agents"), as well as content directly emanating from designated terrorist organisation. Similar risks have been noted as well generally for violent groups that are not designated as terrorist organisations (e.g. violent criminal organisations, religious or political extremist groups). Risks related to the dissemination of content from sanctioned entities have also been observed by providers and CSOs.

Examples of **risk factors** concerning systemic risks related to **terrorist, violent groups and sanctioned entities**:

Design and features: Certain features may increase the risk that terrorist actors can disseminate propaganda, recruit followers, or coordinate activities. For example, livestreaming functionalities have been identified by some providers as potentially enabling real-time dissemination of content associated with terrorist acts.

Monetisation policies and their enforcement: Some CSOs emphasised that monetisation policies may facilitate the dissemination of content from terrorist groups and EU-sanctioned entities.

Examples of **observations by providers and CSOs** concerning systemic risks related to **terrorist, violent groups and sanctioned entities:**

X, 2025 DSA risk assessment report, p. 25: *"The inherent risk of dissemination of terrorist content on X arises from the potential for individuals or groups who use the platform to disseminate terrorist and extremist propaganda, recruit followers, facilitate or coordinate violent attacks, solicit funds from sympathisers, and praise, support, or glorify terror attacks"*.

"NEVER AGAIN" Association, a CSO specialised on human rights, as cited in the report submitted by Appeal Centre Europe, noted the existence on VLOPs and VLOSEs of *"content praising or justifying violent acts carried out by violent extremists, criminal, or terrorist organisations,* [as well as] *content that depicts the insignia, logos or symbols of violent extremist, criminal, or terrorist organisations in order to praise or promote these organisations"*.

3.1.4. Illegal hate speech and the incitement of hate crimes

VLOPs and VLOSEs providers, in particular social media, porn platforms and search engines, have identified risks related to illegal hate speech and the incitement of hate crimes. Several providers have identified illegal hate speech as a risk associated with systemic risks related to other areas, such as the fundamental rights to freedom of expression and non-discrimination, gender-based violence and public security.

DEFINITIONS OF ILLEGAL HATE SPEECH. 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/JHA10, namely race, colour, religion, descent, or national or ethnic origin.

Multiple providers of social media define illegal hate speech as speech that incites violence and that targets a person or a group based on their protected characteristic(s) and referring to them in degrading ways, by using slurs or comparisons to criminals, inanimate objects and denying or minimising events such as the Holocaust and genocide. In addition to illegal hate speech, providers also reported on hate speech they prohibited in their own terms of service (e.g. several providers also include categories such as sexual orientation, disability, or extreme misogyny content insofar as it can be linked to other risks such as gender-based violence).

OFFLINE REPERCUSSIONS OF ILLEGAL HATE SPEECH ONLINE. Some CSOs highlighted that online illegal hate speech may translate into offline harm, including physical violence, harassment, and discrimination, including GBV. Some providers and CSOs stressed that occurrences of illegal hate speech online may have wide ranging consequences and result in other sets of risks (e.g. on mental health, public security) that affect not only the victims of that hateful speech but also wider audiences who may be exposed to it involuntarily. Some CSOs highlighted spikes in gendered or LGBTQI+-focused illegal hate speech during, for example, pride events. Likewise, some CSOs mentioned that illegal hate speech, in particular against minorities, tends to increase around electoral periods or crisis events such as mass killings.

OUT-OF-COURT DISPUTE SETTLEMENT. Some CSOs noted that while implementing the independent decisions taken by out-of-court dispute settlement bodies is not a legal requirement under Article 21 DSA, low implementation rates can increase the risk of illegal hate speech and incitement to violence disseminating on platforms.

Examples of **risk factors** concerning systemic risks related to **illegal hate speech and the incitement of hate crimes**:

Content moderation. The way illegal hate speech manifests on platforms constantly evolves as actors change tactics to circumvent enforcement, as highlighted by some social media providers. Some social media providers and CSOs also highlighted that illegal hate speech, if not detected by content moderation systems, may spread virally to wide audiences, thus contributing to the normalisation of illegal hate speech online.

Specific regional or linguistic aspects: Some social media providers and CSOs identified specific regional or linguistic aspects as a risk factor, highlighting challenges in recognising content as illegal hate speech due to highly localised contexts, such as language influenced by regionally-evolving terms or coded language and symbols. These aspects pose content moderation challenges and were also brought up by CSOs.

AI systems: The possibility to create and disseminate AI-generated images, videos and audio increases the risk of dissemination of illegal hate speech, particularly when they are disguised using coded language, as some social media providers highlighted.

Recommender systems: Some social media providers mentioned that the design of their recommender systems may expose users to hateful content. Some CSOs highlighted that the design of recommender systems, specifically if optimised for user engagement, might amplify illegal hate speech.

Design and features: Some providers acknowledged that features such as anonymous profiles, direct messaging and the ability to tag users can increase the risk of illegal hate speech. Some CSOs argued that such other features may encourage illegal hate speech, for example short, dynamic visual content, which can lead to rapid and emotional reactions, including intensive interactions in the comment sections of short videos. At the same time, the possibility to express oneself anonymously online is an important safeguard for the right to freedom of expression.

Examples of **observations by providers and CSOs** concerning systemic risks related to **illegal hate speech and the incitement of hate crimes**:

X, 2025 DSA risk assessment report, p. 28: *"Features such as Spaces and Communities, anonymous profiles, direct messaging, and user tagging; as well as external events can increase the inherent risk of hate speech on X"*.

DigiQ, a CSO specialised on hate speech, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"The online environment is an integral part of public life. Alongside providing space for creativity, self-expression, and connection, it also enables the dissemination — and often amplification — of hateful narratives present in offline society. Online hate speech has real consequences for users' dignity, mental health, and safety, and cannot be reduced to a purely virtual problem"*.

Snapchat, 2024 DSA risk assessment report, p. 51: *"As explained in the Terms section of this Report, "hate speech" as defined in Snap's Community Guidelines, includes both illegal and legal but harmful speech. As such, Snap's definition of hate speech is more inclusive than most legal definitions of hate speech, because Snap wants to tackle harmful (but) legal speech as well"*.

Pinterest, 2025 DSA risk assessment report, p.22: *"Hateful activities include slurs and negative stereotypes, caricatures and generalisations, as well as support for hate groups and people promoting hateful activities"*.

3.1.5. Intellectual property ("IP") rights violations

While the majority of providers of online marketplaces including app stores have identified risks linked to the dissemination of IP-infringing products, pornographic platforms, search engines, and social media have also highlighted risks related to the dissemination of IP-infringing content. IP rights violations risks also intersect with other risk areas, such as consumer protection (e.g. in the context of counterfeit goods). Furthermore, app stores may be used to disseminate copycat apps and/or apps that distribute content that violates IP rights, such as pirated works (e.g. music, audiovisual works, such as sports and other live events, video games, visual art such as photographs and paintings) as well as to facilitate access to illegal streaming services and products. Moreover, ratings and reviews may also be used to engage in IP infringement.

Examples of **risk factors** concerning systemic risks related to **intellectual property rights violations**:

AI systems: Some providers have reported that, as AI tools become more widespread and generative AI models become more developed, users may increasingly produce and disseminate on VLOPs and VLOSEs content that reproduces existing works or incorporates creators' intellectual property without their authorisation.

Content moderation systems. The over-enforcement of IP rights has been mentioned by some providers as amplifying other risks for example by suppressing lawful expression of artists and content creators. In this context, content reporting mechanisms may be misused by users to falsely flag content as infringing EU law in order to silence others, while rightsholders themselves may use infringement claims in an abusive manner to defame others.

Examples of **observations by providers and CSOs** concerning systemic risks related to **intellectual property rights violations**:

Shein, 2025 DSA risk assessment report, p. 31*: "We have analysed the risk of IP infringing and counterfeit products being offered on the Marketplace and found that if unmitigated, this risk would materialise if Sellers, for example: 1) Used the Marketplace to list, publish and sell products that infringe someone's IP, such as selling fake designer clothes or handbags (i.e. counterfeit) at the designer's price or less; or 2) Used the Marketplace's functionalities to list and publish products under the trademark of a third party"*.

Temu, 2025 DSA risk assessment report, p. 29: *"The IP risk sub-module assesses the risk that traders may use Temu to disseminate products that infringe third parties' IP rights, including*

trademarks, copyrights, patents, and design rights defined under applicable laws of the EU and the EU Member States".

Stripchat, 2024 DSA risk assessment report, at p. 30, mentioned a risk of: *"Stripchat users, visitors, models, studios or advertisers directly or indirectly using Stripchat for uploading, streaming, sharing links to or otherwise facilitating* [intellectual property rights] *infringements, resulting in violation of the applicable EU laws"*.

3.2. Negative effects on fundamental rights

Article 34(1)(b) DSA requires that DSA risk assessments cover *"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"*. Drawing on the risk assessment reports submitted by VLOPs and VLOSEs providers, as well as observations from public interest stakeholders including CSOs and academia, this Section offers an overview of systemic risks concerning a selection of the fundamental rights referenced in Article 34(1)(b) DSA.

Article 35 DSA requires that providers of VLOPs and VLOSEs adopt measures that are reasonable, proportionate and effective, and that such measures be designed with particular regard to their potential impact on fundamental rights, including the right to freedom of expression and information, which is a point further emphasised in recital 86 DSA. Transparency obligations regarding content moderation provide an additional layer of protection: Articles 15, 16 and 24 DSA require providers of online platforms to give statements of reasons for content moderation decisions and to report publicly on their content moderation practices. Furthermore, Article 8 DSA prohibits the imposition of general monitoring and active fact-finding obligations on providers of online platforms and search engines, thereby safeguarding a variety of fundamental rights, including freedom of expression and information, the right to private and family life and the right to the protection of personal data. Generally, the DSA provides users and organisations with a range of tools and redress mechanisms to be informed of and challenge content moderation decisions, including through internal complaint-handling systems and certified Out-of-Court Dispute Settlement bodies.

Both providers and CSOs have flagged systemic risks relating to fundamental rights, though the specific rights at stake and the nature of those risks differ considerably across platform types.

3.2.1. Right to freedom of expression and information

VLOPs and VLOSEs such as social media and search engines have been highlighted as the most relevant with regard to risks related to the fundamental rights to freedom of expression and information. Systemic risks to the fundamental rights to freedom of expression and information are relevant to many other risk areas, such as illegal hate speech, negative effects on the fundamental right to non-discrimination, civic discourse, electoral processes and public security, as well as gender-based violence and public health. 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 fundamental right to freedom of expression and information. The first edition of Article 35(2) report published on 18 November 2025 highlighted the importance of the DSA's risk management framework as a key safeguard for fundamental rights, 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 rather 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), either due to an over-enforcement of content moderation policies or due to an unsafe online environment creating chilling effects on free expression (e.g. due to illegal hate speech or gender-based violence).

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

Content moderation systems: Risks of over-moderation have been mentioned by providers and CSOs, for example by emphasising that automated content moderation systems may misinterpret context, nuance, or cultural references, increasing the risk of producing "false positives", leading to lawful and compliant content or accounts being removed or restricted. Providers mentioned that human review is subject to error as well, and that even trained moderators may make mistakes, display personal, cultural, political, or contextual biases, or face limited resources. Providers and CSOs also mentioned that an unsafe online environment due to a lack of effectiveness of content moderation systems may result in chilling effects on the right to freedom of expression, for example when public figures, especially women, are harassed, intimidated or defamed online, including through the use of deepfakes.

Intentional manipulation of the services: Abusive reporting may include mass reporting campaigns designed to trigger enforcement actions, or, abusive intellectual property notices

intended to suppress competition. Such practices exploit enforcement mechanisms, create additional burdens for platform providers that may result in restrictions and removal of compliant content or accounts. Coordinated disinformation campaigns aimed at manipulating the information environment could negatively affect media pluralism and thereby interfere with the right to freedom of expression.

AI systems: According to providers and CSOs, generative AI could be used to spread misinformation and disinformation and introduce bias into online conversations, affecting freedom of expression and information.

Monetisation policies and their enforcement: Some CSOs highlighted that content monetisation restrictions, if enforced arbitrarily, may contribute to risks of chilling effects on the right to freedom of expression, because when monetisation is a primary income source, creators and media outlets may avoid certain topics, positions, or language to reduce the risk of demonetisation or reduced reach.

Examples of **observations by providers and CSOs** concerning systemic risks related to the **fundamental rights to freedom of expression and information**:

Facebook, 2025 risk assessment report, p. 93-94: *"This* [systemic risks to freedom of expression] *can manifest on Facebook through over-enforcement of non-policy-violating content, disproportionate enforcement of policy-violating content, language/dialect limitations of human reviewers or classifiers, failure to take down policy-violating content, activity that limits or discourages a users' freedom of expression, and the inherent difficulty in balancing freedom of expression and safety concerns".*

Wikipedia, 2025 DSA risk assessment report, row 2: *"Actors interested in a particular political/electoral/civic outcome could launch coordinated campaigns to insert misleading content into Wikipedia, reducing the broader reliability of content, misleading readers, and spreading disinformation"*.

EFCSN, the association of European fact-checking organisations, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"By flooding communication spaces with falsehoods or inauthentic content, the freedom of expression of EU citizens is unfairly limited as their speech might be drowned out by inauthentic speech (e.g. from bots or sockpuppets)"*.

3.2.2. 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, pornographic platforms and search engines. These systemic risks are related to other areas such as illegal hate speech, gender-based violence or the protection of minors.

DISCRIMINATION IN GENERAL. Providers and CSOs mentioned systemic risks related to the promotion of discriminatory views, in particular vis-à-vis specific groups based on their gender, racial ethnic or cultural origin, religion or belief, disability, age or sexual orientation. Some CSOs reported discrimination risks linked to the dissemination of content that promotes racial and religious discrimination, and, in some cases, violence against minority communities. Some CSOs mentioned discrimination risks related to the dissemination of harmful narratives comparing minorities to animals, monsters, uncontrollable forces of nature such as floods, drawing on tropes of invasion and contamination to generate fear and moral panic. Some CSOs mentioned "dog whistle" risks where coded language and references to seemingly innocuous objects and images have acquired violent connotations and are used to evade content moderation.

ACCESSIBILITY BARRIERS IN PARTICULAR. Some providers and CSOs mentioned that accessibility barriers may pose risks of non-discrimination when platform services, features, or information (e.g. functionality, product listings, or terms and conditions) are not equally accessible to users with disabilities, limited digital literacy, or diverse linguistic backgrounds. This may lead to the exclusion of vulnerable groups.

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

Recommender systems. Some CSOs observed that recommender systems may amplify discriminatory content or systematically disadvantage certain groups by differentially exposing them to content.

Content moderation. Some CSOs identified gaps in non-English capabilities of providers' content moderation systems. In particular, automated moderation systems were observed by some CSOs having limited capacity to detect coded speech, cultural references, sarcasm, and text embedded in images in certain languages, including minority languages of foreign diasporas established in the EU, in which, for example, visual propaganda and AI-generated content may bypass detection mechanisms.

Monetisation policies and their enforcement. Some CSOs noted that certain VLOPs' monetisation policies may have negative effects on fundamental rights, notably by enabling

the dissemination of content which may fuel discrimination against minority voices and media.

Examples of **observations by providers and CSOs** concerning systemic risks related to the **fundamental right to non-discrimination**:

DAHRD, a CSO specialised in the fight against discriminations, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Targeted individuals and communities are exposed to public humiliation, stereotyping, and coordinated harassment, leading to social exclusion and segregation. These dynamics produce chilling effects on online participation, discouraging civic engagement and self-expression. Overtime, the persistent digital environment of hostility increases offline risks, including discrimination, intimidation, and violence, undermining dignity, security, and equal participation in public life"*.

Bing, in its 2025 DSA risk assessment at p. 69 mentioned a: *"Risk that content or activities with actual or foreseeable negative effect on the fundamental right to non-discrimination occur on the service, impacting individuals and groups based on race, ethnicity, religion, gender, sexual orientation, or other protected traits, or reflecting, reinforcing, or perpetuating harmful stereotypes, biases, or inequalities".*

Booking, in its 2025 DSA risk assessment report at p. 32 mentioned a: *"Risk that services or features on the platform may not function equitably for users with certain disabilities or limited digital literacy (non-discrimination).* [...] *Users with disabilities or digital literacy challenges may face barriers when accessing and utilizing our platform, potentially leading to an inequitable user experience and limiting their travel options"*.

3.2.3. Rights of the child

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

3.2.4. Consumer protection

Providers of VLOPs and VLOSEs such as online marketplaces, pornographic platforms and social media are the most relevant with regard to risks related to the fundamental right to consumer protection. Consumer protection risks are closely related to other systemic risk areas such as the dissemination of illegal or non-compliant products, IPR violations, public health and physical well-being.

FAKE ENGAGEMENT, FAKE REVIEWS. Providers and CSOs have noted systemic risks resulting from fake engagement, including fake or manipulated reviews, for example from bots, which may affect consumers' choices by limiting their ability to distinguish authentic from inauthentic feedback as they can inauthentically inflate ratings, reviews, or sales volume, in collusion with sellers. In the same context, risks related to merchant impersonation as well as the misrepresentation of business or product information have also been highlighted by online marketplaces.

SCAMS. Systemic risks related to scams have been underlined by providers and CSOs. Such systemic risks also concern more stakeholders beyond only consumers. These include financial scams (which can manifest in sectors such as high risks financial products and investments, Ponzi schemes, betting, unregulated gambling, lotteries, cryptocurrencies, foreign real estate, tax rebates, energy savings, giveaways) as well as other types of scams (e.g. romance scams, health supplements, dating services, clairvoyance services). Systemic risks related to financial scams, in particular in the context of advertisement (as described further in the text box on risk factors below), have been identified by a wide range of stakeholders, including providers, CSOs as well as Members of the Board as amongst the most prominent and recurrent systemic risks identified during the reporting period. Information sources such as the advertisement repositories from Article 39 DSA have in this context provided valuable insight to identify such systemic risks. Members of the Board noted some of the following techniques as having been used to disseminate scams on VLOPs and VLOSEs:

- Deceptive endorsements: User comments/reviews with stock images or AI-generated content, plus "experts"/"doctors" or "awards/certifications" presented without verification;
- Frequent use of out-of-context scientific vocabulary to inflate apparent credibility (e.g. "nanotechnology", "astronauts' secret formula");
- Opacity regarding manufacturer/ingredients (e.g. vague legal entities, lack of concrete details);
- Template reuse across products/markets (e.g. identical page structures, identical efficacy narratives and "treatment timelines");
- Official symbol misuse such as the use of state emblems/logos or invocation of health authorities to confer false legitimacy to illegal products or services;
- Aggressive sales and subscription traps such as fake countdown timers, "last items", flash discounts, buried subscription terms, and other pressure tactics to trigger impulsive purchases.

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

AI systems. Some CSOs mentioned that financial scams may be facilitated by the use of generative AI, for example due to deepfakes imitating public figures giving fake endorsements.

Advertising systems. Some providers and CSOs noted that advertising systems may be misused to promote investment scams. Some CSOs noted that removing individual scam advertisements while leaving scam accounts and scam networks in place, allows the same actors to continue or resume operating. Some CSOs noted that certain scammers use advertisements to redirect users off-platform. Some providers mentioned the risks that advertising systems may display advertisements that include AI-generated content representing illegal activities such as adult sexual abuse.

Monetisation policies and their enforcement. Likewise, some CSOs emphasised that in certain cases monetisation policies and their enforcement may contribute to fraud by incentivising content creators to produce scams, for example when influencers benefit from affiliate programmes and engagement-based payouts when disseminating harmful content such as scams.

Examples of **observations by providers and CSOs** concerning systemic risks related to the **fundamental right to consumer protection**:

Amazon, 2025 DSA risk assessment report, p. 25: *"Most recently an illicit industry has developed with Fake Reviews brokers looking to profit by offering, procuring, selling, or hosting public and private groups on third party sites where Fake Reviews are exchanged for compensation. These brokers approach consumers directly through websites, social media channels, and encrypted messaging services, soliciting them to write Fake Reviews in exchange for money, free products, or other incentives"*.

Booking, in its 2025 DSA risk assessment report a p. 35 mentioned a: "*Risk that geo-pricing on the platform may result in unjustified discrimination (consumer protection). Customers located in the European Economic Area (EEA) have access to the same content, prices and conditions on Booking.com. Supply partners are restricted from "geo-pricing" (e.g. offering different prices based on travellers' geographical location) within the EEA"*.

3.2.5. Rights to private and family life and personal data protection

Providers of VLOPs and VLOSEs such as social media, app stores and pornographic platforms are the most relevant with regard to risks related to the fundamental rights to private and family life and data protection. Other risks are relevant to systemic risks to private and family life and data protection, for example risks to the protection of minors, risks of gender-based violence, or mental well-being. Providers and CSOs have identified risks arising from users relying on a provider's services to infringe upon the rights to private and family life and to data protection of other users, for example through stalking, doxxing and the dissemination of surveillance apps. For example, surveillance apps being available on app stores that are designated VLOPs have been mentioned by CSOs as being used by abusive partners to commit violations of privacy to facilitate gender-based violence. Providers also emphasised risks from inadvertent disclosure of private or location-based data. CSOs highlighted the social pressure children are under to publish personal information to engage on social media platforms.

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

AI systems: Some CSO noted that generative AI nudifying apps and the dissemination of related content via VLOPs and VLOSEs create risks to the rights to private and family life and data protection of the persons who are depicted in such content.

Monetisation policies and their enforcement: Some CSOs highlighted risks to the privacy of children whose images and videos are being shared online, for instance, by parent influencers, in particular due to the monetisation policies of certain providers which create financial incentives to produce and disseminate such content.

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

XVideos, 2025 DSA risk assessment report, p. 20: *"Given the delicate nature of user data, which often involves private viewing histories (where enabled by the user), and personal data/information, the consequences of privacy breaches can be particularly severe. Given the stigma, risks, and personal nature of adult content consumption, users are susceptible to the security of their personal data. Leaked viewing histories can lead to personal embarrassment, blackmail, or financial fraud, making privacy concerns uniquely high stakes for an adult platform"*.

Bundersverband Frauenberatungsstellen und Frauennotrufe (bff), submission to the invitation for contributions from the European Board for Digital Services and the European

Commission: *"Advertising systems can indirectly contribute to GBV by facilitating the promotion of tools enabling abuse. Examples include advertising for* [...] *applications that generate sexualised deepfakes, services that manipulate images without consent, surveillance tools used for stalking".*

3.3. Negative effects on civic discourse, electoral processes, and public security

Under Article 34(1)(c) DSA, risk assessments must cover *"any actual or foreseeable negative effects on civic discourse and electoral processes, and public security"*. This Section sets out the main systemic risks in this area as identified by VLOPs and VLOSEs providers and CSOs.

How these risks manifest depends on the nature and function of each service, the behaviours it enables, and the broader societal context in which it operates. The implications for civic discourse on a search engine, for instance, differ considerably from those arising on an online marketplace. In their risk assessment reports, many providers considered the role of misinformation and disinformation when evaluating potential negative effects on civic discourse, electoral processes, and public security, though definitions of these terms vary across providers. For the purposes of this report, the definitions set out in the European Democracy Action Plan are used: disinformation refers to *"false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm"*, while misinformation denotes *"false or misleading content shared without harmful intent though the effects can still be harmful"*. Several VLOPs and VLOSEs providers have, through the Code of Conduct on Disinformation, committed to building on these definitions. Under that Code, the term "disinformation" is used by signatories to encompass misinformation, disinformation, information influence operations, and foreign interference in the information space.

The systemic risks presented in this Section do not concern individual pieces of content, but the design, operation, and large-scale use of services. In that context, algorithmic content recommendation systems and content ranking mechanisms are particularly relevant, as are artificial intelligence features such as AI-generated content summaries that have been incorporated into the services of certain providers. Content moderation and information integrity systems, including the use of fact-checking mechanisms, are likewise relevant insofar as their design, coverage, and effectiveness may influence systemic risks in relation to civic discourse, electoral processes, and public security.

Finally, systemic risks to well-functioning civic discourse do not exist in isolation; rather, they are inextricably tied to the fundamental rights of users, including the right to freedom of expression and information (see Section 3.2). As such, any mitigation measures that would be taken to mitigate systemic risks to civic discourse, electoral processes, and public security need to be balanced against the right to freedom of expression and information. The risk category

of systemic risks to civic discourse and electoral processes is not a catch-all category that would be broadly relevant where the dissemination of user speech could make civic discourse unpleasant or adversarial. Rather, especially in cases of lawful speech of a political nature, it is an integral part of civic discourse to tolerate opposing views, including lawful statements that some may consider controversial. Therefore, the risk mitigation measures appropriate for this category of systemic risks need to be taken with particular care for the right to freedom of expression. The risk mitigation measures appropriate for this category of systemic risks must reflect respect for fundamental rights, including the right to freedom of expression, which includes the right to receive and impart information on politically sensitive topics.

3.3.1. Civic discourse and electoral processes

Providers of VLOPs and VLOSEs such as social media and search engines are the most relevant with regard to risks related to voting and electoral processes. This risk area intersects with others such as systemic risks related to the right to freedom of expression and information, illegal hate speech, terrorist groups, violent groups and sanctioned entities, as well as gender-based violence.

ELECTORAL PROCESSES. Systemic risks related to disinformation and misinformation about voting and electoral processes have been mentioned by providers and CSOs. These covered for example the large-scale dissemination of incorrect dates for voter registration or for elections time and dates, or of baseless claims of elections fraud or of cancellations of elections, as well as the large-scale dissemination of incorrect information about eligibility criteria for voters or about how to correctly fill out a ballot or use mail-in voting. Some CSOs reported electoral process risks related to the dissemination of voting booth footages, which is illegal in certain Member States. More generally, disinformation related to harmful conspiracy theories and the large-scale dissemination of falsely authoritative content have also been mentioned by CSOs and providers. Some CSOs and providers mentioned that civic discourse risks are particularly acute during electoral periods but remain also relevant outside of such periods. Some CSOs noted in particular that risks related to civic discourse and electoral processes do not only affect adults or users with the right to vote but also minors which are still in the process of developing their personality, as for example disinformation decreases trust in public authorities also in the eyes of minors.

PUBLIC FIGURES HARASSMENT. Providers and CSOs mentioned risks related to harmful personal attacks (including defamation or harmful conspiracy theories), doxxing, hate speech, etc. attacking public figures. Reported types of individuals and organisations concerned by this systemic risk included: politicians or political candidates, civil servants, government officials, business leaders, journalists, celebrities, scientists (notably those working on political, geopolitical, climate or public health issues), representatives of CSOs, trusted flaggers and fact checkers.

VOTER HARASSMENT. Voter intimidation and harassment are identified by providers and CSOs as systemic risks arising from misleading information, coercive messaging, or coordinated harassment targeting voters.

FIMI. Foreign Interference and Information Manipulation (FIMI), including coordinated inauthentic behaviour, both on- and off-platform have been identified by both providers and CSOs as a systemic risk to civic discourse and electoral processes.

Examples of **risk factors** concerning systemic risks to **civic discourse and electoral processes**:

AI systems: Some CSOs observed that AI chatbots may disseminate mis- and disinformation and that they may be manipulated. Some CSOs also noted that there is an exponential increase in the use of generative AI content to create realistic fake content with the aim of influencing civic discourse; for example, generative AI systems may contribute to risks related to the impersonation of public figures, leading potentially to defamation, as well as of ordinary people, leading potentially to harassment and voter intimidation.

Monetisation policies and their enforcement: Some CSOs mentioned that some risks to civic discourse might be amplified by monetisation policies financially enabling the dissemination of mis- and disinformation.

Intentional manipulations of the services: Some CSOs mentioned how coordinated inauthentic behaviour, including resulting from FIMI, may contribute to negative impacts on civic discourse and electoral processes. Some CSOs mentioned specifically risks of coordinated services manipulation campaigns being carried out from outside of the EU for example by botnets to influence electoral processes in the EU. Some CSOs noted how inauthentic behaviour linked to the dissemination of mis- and disinformation may be carried out across several platforms.

Recommender systems: Some CSOs highlighted that restrictions on the visibility of political content may contribute to risks to civic discourse, stating that the right to freedom of expression on VLOPs and VLOSEs does not only entail the ability to post, but also the ability to be seen online.

Examples of **observations by providers and CSOs** concerning systemic risks to **civic discourse and electoral processes**:

Fundación Maldita.es, a CSO specialised on disinformation matters, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"The risk presented by AI-generated disinformation has increased exponentially*

during the last period. With the improvement of the quality of the outputs produced by AI models, these tools are being used to produce realistic content linked to current world events, displacing legitimate coverage and shaping public opinion".

Democracy Reporting International, a CSO specialised on electoral matters, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"*[M]*ultiple LLM chatbots produced inaccurate, misleading, or entirely fabricated information about candidates, parties, electoral procedures, and voting eligibility. None of the systems consistently redirected users to authoritative sources such as official electoral authorities websites. These failures occurred across standard use cases (e.g., users asking basic electoral questions) meaning the risk is not confined to adversarial or edge-case interactions but embedded in routine platform functionality"*.

EFCSN, the association of European fact-checking organisations, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"The monetization of polarizing and misleading content on social media is driven by engagement-based revenue models that reward virality rather than accuracy. These incentive structures favour emotionally charged and divisive narratives, which are systematically amplified through algorithmic recommendation systems"*.

XNXX, in its 2025 DSA risk assessment report p. 19: *"*[C]*ross-linkages with civic and advertising risks reveal how sexualised disinformation and gender-harmful advertising extend gender-based violence beyond content into broader social and economic structures. Taken together, these patterns confirm gender-based violence as pervasive, cross-cutting systemic risk"*.

X, 2025 DSA risk assessment report, p. 51: "*Risks to democratic processes, civic discourse, and electoral processes may arise from false or misleading information, voter intimidation and/or suppression, presence of hateful entities"*.

3.3.2. Public security

Providers of VLOPs and VLOSEs such as social media and search engines are the most relevant with regard to risks related to public security. Other areas of risks are also relevant to public security risks, such as content from terrorist groups, violent groups and sanctioned entities, illegal hate speech and the incitement of hate crimes. Examples of systemic risks to public security identified by providers and CSOs included the dissemination of content that praises, incites or glorifies riots, civil unrest, or criminal acts against individuals or property, including state or public infrastructure, as well as the 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. Likewise, there have been mentions of instances

where old content was repurposed, such as videos of bombings, mass shootings or large protests, and framed as real time events with the aim of triggering public panic or inflaming tensions, which may be challenging for providers of VLOPs and VLOSEs to detect or ascertain, especially when the content has been manipulated. Furthermore, risks to public security have been mentioned by providers and CSOs in relation to crises and disasters: for example, the dissemination of disinformation or content that may cause panic, hoarding behaviour (e.g. imminent collapse of essential services (e.g. food supply chains, running water, fuel, or access to cash dispensers)). Examples of the types of crises and disasters concerned by this systemic risk included violent events, such as shootings, mass murders, terrorist attacks or armed conflicts, natural crises such as floods, earthquakes, wildfires, hurricanes, landslides, as well as other types of crises such as industrial accidents, public health crises, climate change.

Examples of **risk factors** concerning systemic risks to **public security**:

Recommender systems: Recommender systems may pose risks to public security by amplifying harmful or unlawful content before it is detected or flagged, thereby increasing its visibility and reach. During crises, armed conflicts, or public emergencies, such amplification may contribute to the spread of harmful misinformation, extremist propaganda, terrorist recruitment material, or content inciting violence. By prioritising engagement-driven or personalised content, recommender systems may also unintentionally elevate adversarial actors, reduce exposure to pluralistic sources, and facilitate coordinated disruptive activities, potentially affecting public security.

AI systems: Providers and CSOs emphasised the role of generative AI as a risk factor to systemic risks to public security, for example in the context of the creation of fake content intended to stoke violence.

Examples of **observations by providers and CSOs** concerning systemic risks related to **public security**:

Instagram, 2025 DSA risk assessment report, pp. 18 and 21: *"Foreign influence operations* […] *and cross-internet Coordinated Inauthentic Behaviour (CIB) campaigns have continued to persist as a trend on the platform"* […] *"For our assessment of Public Security risks in 2025, we identified that the risk landscape could be impacted by continued trends that Meta monitors around EU elections and GenAI advancements. We have also observed ongoing trends related to violent and graphic content shared in the EU"*.

LinkedIn, 2025 DSA risk assessment report, p. 75: "*Risk to Public Security includes risk that content or activities degrading public security occur on the platform including terrorist recruitment, funding, or training activities, terrorist imagery or content, or support for*

terrorists or glorification of terrorist acts as well as mis- or disinformation related to crisis events. Absent sufficient mitigations, risks related to Public Security may manifest on the platform in ways such as the members posted content glorifying terrorist acts in Feed, members posting a job that facilitates terrorist activities, or advertisers promoting content with misinformation on a public crisis event".

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

Article 34(1)(d) of the Digital Services Act (DSA) requires providers of VLOPs and VLOSEs to 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 individuals' physical and mental well-being*". These risks are context-dependent, varying across services, societal environments, and patterns of user behaviour. Risks related to GBV and the protection of minors are also relevant to other risk categories, including mental and physical well-being, civic discourse and fundamental rights.

3.4.1. Gender-based violence ("GBV")

Providers of VLOPs such as social media and pornographic platforms are the most relevant with regard to risks related to GBV. GBV has been closely associated by providers and CSOs with other systemic risk categories, including illegal content such as adult sexual abuse material and infringements of the fundamental right to non-discrimination, as well as risks to personal safety, thereby intersecting with further risk categories such as mental and physical well-being. One of the key objectives of the EU Gender Equality Strategy 2020-2025 is to end GBV in all its forms, including online violence[14]. The Directive on combating violence against women and domestic violence criminalises different forms of cyber violence: the non-consensual sharing of intimate or manipulated material (including by means of artificial intelligence), cyber stalking, cyber harassment, cyber flashing and cyber incitement to violence or hatred[15]. This was also highlighted in the Union of Equality LGBTIQ+ Equality Strategy 2026-2030[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

[14] 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.

[15] 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. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 14 June 2027.

[16] 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.

intermediary services has contributed to the emergence and amplification of gender-based cyber violence.

HARASSMENT AND GENDERED HATE. Providers mentioned that GBV may occur through a wide range of platform features, including comments, direct messages, reviews or user-generated posts, and can also involve the promotion of products or content that glorifies violence or discrimination against individuals on the basis of gender. The harms of gender-based harassment extend beyond isolated incidents, leading to psychological distress, reputational and economic damage, and potential threats to physical safety, while repeated exposure may reinforce structural inequalities and deter participation in online spaces, silencing the victims. Providers and CSOs noted that, for example, LGBTQ+ individuals, and female public figures may face elevated levels of gender-based harassment on platforms. Gender-based harassment frequently occurs in sexualised forms, such as unwanted sexually explicit or degrading messages directed at individuals on the basis of their gender. Such behaviour may for example materialise through commercial features such as listings and reviews, where user-generated content may contain abusive messages, sexual harassment against women or men, or gender-based slurs.

EXTREME MISOGYNY CONTENT AND FREEDOM OF EXPRESSION. Some providers and CSOs noted that coordinated harassment can create hostile online environments that discourage participation and silence targeted individuals or communities as affected users may withdraw from discussions or reduce their engagement in online spaces. Female politicians, for example, have been mentioned by providers and CSOs as being disproportionately subject to harmful and hateful comments, which can undermine freedom of expression, and the diversity of viewpoints present on platforms, as individuals who experience abuse may engage in self-censorship or leave the platform entirely. Also, platforms recognise the risk of fake accounts being used with the intend to silence, harass or discredit survivors of GBV, which in turn can lead to re-traumatisation.

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

Recommender systems: Providers have highlighted that engagement-driven recommendation systems may inadvertently amplify harmful or policy-violating content, including GBV content. Where algorithmic ranking prioritises interaction metrics over safety considerations, such systems may increase the visibility and societal normalisation of gender-based violence. Furthermore, providers and CSOs noted that discrimination can be a consequence of biased algorithmic systems. CSOs noted risk factors such as algorithms that amplify and monetise misogynistic content, coordinated harassment campaigns, gender-based disinformation, intimidation and targeted abuse against women in public life (weaking

their participation in democracy). These risks may normalise gender inequality, reinforce societal biases, impact rights, and may result in offline harm.

Content moderation systems: Providers noted that insufficient detection tools, delayed takedown procedures, or ineffective reporting systems can allow GBV content to persist online. Gaps in moderation capacity or enforcement consistency may therefore increase both the duration and severity of harm, particularly where victims lack accessible and timely remedies. Some providers noted that the abusive use or malfunctioning of content moderation systems may lead to the silencing or censoring of affected individuals and groups.

AI systems: Providers have acknowledged that generative AI tools lower the barriers to creating realistic, manipulated, or synthetic content, including AI-generated non-consensual imagery. This technological development increases the scalability and sophistication of GBV content and may complicate detection and attribution efforts of such content. Independent researchers have also emphasised the serious risks posed by the non-consensual sharing of private images, particularly those created with AI systems, disproportionately affecting women. Synthetic materials like deepfakes or content generated through "nudification" and disseminated on online platforms, may increase risks of gender-based violence by facilitating the non-consensual sharing of private images. Some CSOs noted that AI tools embedded in VLOPs and VLOSEs may be used to disseminate CSAM, deepfake nudes and sexualised violence against women.

Design and features: Platform features (such as messaging or location-sharing) can be misused to control or monitor victims, especially in domestic violence contexts. At the same time, content moderation may fail to capture context-dependent abuse (e.g. repeated behaviour or implicit threats), leaving some forms of GBV insufficiently addressed.

Intentional manipulation of the services: Beyond individual instances of abuse, systemic risks may also arise from coordinated forms of harassment in which multiple actors collectively target individuals or groups. Such behaviour may involve organised campaigns, brigading or repeated unwanted contact carried out by adversarial networks, sometimes operating across multiple accounts or platforms.

Examples of **observations by providers and CSOs** concerning systemic risks related to **gender-based violence**:

TikTok, 2025 DSA risk assessment report, p. 43: "*The risks relating to GBV may arise from users attempting to share or disseminate content depicting or involving the following types of behaviour on or through the Platform, including through video or photo, livestream, comments, profile information or TikTok Shop features:*

- *Non-consensual sexual acts that are real or fictional including rape, molestation and non-consensual touching;*
- *Image-based sexual abuse ("IBSA"), including AI-generated IBSA, and sextortion;*
- *Sexual harassment;*
- *Gender-based hate speech, including the promotion of violence, exclusion, segregation, discrimination and other harms on the basis of gender, gender identity or sex or certain hateful ideologies, including male supremacy or misogyny;*
- *Violent behaviour where gender is a relevant factor, including intimate partner violence or threatening or expressing a desire to cause physical injury to a person or a group on the basis of gender; and*
- *Harassment and bullying where gender is a relevant factor, such as degrading someone or expressing disgust on the basis of their personal characteristics or circumstances, such as their physical appearance, intellect, personality traits and hygiene (where gender is a relevant factor) (together, "GBV Content").*

TikTok is aware of the risk that users may use fake accounts to post harmful content or harass, silence or discredit victims of GBV".

Bundersverband Frauenberatungsstellen und Frauennotrufe (bff), focusing on fighting against digital violence, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Platform risk assessments often analyse abusive behaviour solely within the boundaries of the platform environment. However, counselling centres consistently observe that digital technologies are frequently used to extend existing patterns of abuse, particularly in situations involving domestic violence, stalking, coercive control, sexual violence"* […] *"Recommender systems optimised for engagement can significantly amplify harmful content and harassment dynamics. Content that generates a strong reaction tends to receive higher engagement, which can lead to increased visibility of abusive or misogynistic content. In cases of image-based abuse or coordinated harassment, algorithmic amplification may contribute to rapid dissemination across networks, thereby intensifying the harm experienced by the survivor"*.

Instagram, 2025 DSA risk assessment report, pp. 22 and 68: *"New and emerging trends have been identified that may impact risks related to adult sexual exploitation (e.g., AI kissing apps, nudification tools, and breastfeeding content)"* […] *"We also recognise that the LGBTQ+ 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 risk can manifest itself on Instagram when adversarial networks work together to engage in repetitive behaviour, which is challenging to identify and manage, as brigading and coordination of mass harassment happen on and off the platform and can take various forms"*.

XNXX, 2025 DSA risk assessment report, p. 26: *"Algorithms designed to maximise engagement may unintentionally prioritise illegal or harmful material, including non-consensual intimate imagery, revenge porn, and deepfakes, or automatically promote new uploads and trending categories without prior moderation review"*.

3.4.2. Public health

Providers of VLOPs and VLOSEs such as online marketplaces, social media and search engines are the most relevant with regard to risks related to public health risks. Systemic risks related to public health often intersect with risks to mental and physical well-being as well as with public security and, in some cases, illegal content.

HEALTH MIS/DISINFORMATION. Several providers and CSOs noted that false or misleading health-related content, resulting from intentional disinformation or unintentional misinformation, or content that maliciously undermines public health institutions, initiatives, or professionals, poses a significant risk to public health and has severe real-world consequences for example during public health crises. In addition, according to some providers and CSOs, there is a risk that low-quality content related to health events is included in news functions, especially during public health emergencies, which could disrupt disaster response. On online marketplaces, including app stores, listing, rating or review functions may also be misused to disseminate content harmful to public health. Content related to self-harm, eating disorders and personal crisis, as well as addiction-facilitating design, also undermines public health, but is discussed in more detail in the section on physical and mental well-being. CSOs observed that highly viral posts promoting unproven and sometimes dangerous treatments were circulating in multiple languages, widely translated and republished.

DISSEMINATION OF HARMFUL PRODUCTS. Another risk for public health is related to harmful products, substances and scams being disseminated or conducted. These can include, for example, dangerous, prescription-only, or stolen medicines or medical devices (e.g. skin-lightening creams with mercury, counterfeit blood pressure monitors), age-restricted products harmful to minors' health (e.g. alcohol, tobacco), or scams disguised as drug sales or other public health-related scams. As with illegal, unsafe, or restricted products, malicious actors use covert ways to evade detection (e.g. signposting).

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

Advertising systems: Providers noted that advertising systems may be a risk factor in promoting harmful products and substances, while CSOs highlighted that insufficient Know Your Business Customer (KYBC) procedures for advertising systems can enable scalable fraud (e.g. in health).

Monetisation policies and their enforcement: Some CSOs noted that the financial incentives, payments and treatments associated with monetisation services can negatively impact public health by incentivising the proliferation of health misinformation, which is easy to autogenerate and need not tied to current events.

Recommender systems: Providers, in particular pornographic platforms, have reported that recommender systems may promote exposure to certain types of content (especially without content warnings or age-appropriate controls) that contribute to unrealistic body image standards that can have adverse effects on the mental and physical health of viewers. These can include issues related to self-esteem, body image, sexual dysfunction, and addiction, potentially impacting users' mental, physical and sexual health. Providers and CSOs noted that the design of certain recommender systems may increase the virality of harmful health-related disinformation and misinformation.

AI systems: Independent researchers have highlighted the growing risk of integrated AI features in online platforms when it comes to health disinformation and misinformation being heightened by user views and engagement, system misinterpretations, and training data. Generative AI also facilitates the generation and spread of unproven health treatments.

Examples of **observations by providers and CSOs** concerning systemic risks related to **public health**:

EFCSN, the association of European fact-checking organisations, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Health misinformation poses a threat not only to individuals' health and wellbeing but also to public health more broadly, and it carries steep economic costs. The most recurring topics exposed to misinformation are cancer treatments, vaccines, their effectiveness, origin and contents and so called wellness trends promoted on social media according to qualitative feedback from our members"*.

LinkedIn, in its 2025 DSA risk assessment report at p. 68 mentioned: "*Risks to Public Health include false information and the promotion of harmful, yet legal, substances or practices (e.g. weight loss medications). Absent sufficient mitigations, risks related to Public Health may manifest on the platform in ways such as members posting misleading health-related information, News results including low quality information related to health events, or LinkedIn Ads promoting legal but harmful substances"*.

3.4.3. Protection of minors

Providers of VLOPs and VLOSEs such as social media, pornographic platforms and search engines are the most relevant with regard to risks related to the protection of minors. The risks to minors vary depending on the platform but are often cross-cutting with risks of various types such as to physical or mental well-being. Due to the substantial overlap between the protection of minors and rights of the child, and given that VLOPs and VLOSEs providers frequently adopt an approach that groups these intersecting areas, the sub-risks are listed below. However, they should be understood as closely interrelated and partially overlapping, particularly where protection concerns directly engage the child's rights. Some of the risks outlined in other Sections of this report also apply to children, they may have heightened implications for minors, given their vulnerability, and may affect them more significantly than adults, e.g. in cases involving consumer protection violations, exposure to harmful content and risks to mental and physical well-being.

COMPULSIVE OR ADDICTION-LIKE BEHAVIOUR ON SOCIAL MEDIA, COMPULSIVE SHOPPING ON ONLINE MARKETPLACES. Some providers noted that minors are particularly vulnerable to extensive, compulsive or addiction-like behaviour due to their stage of cognitive and social development, limited digital literacy, and reduced decision-making capacities. CSOs similarly noted that extensive, compulsive and addiction-like behaviour is a systemic risk. Such compulsive engagement may impair users' autonomy, their control over their time and goals, their sleep, their attentional abilities, and negatively impact their mental and physical well-being. Addiction-like behaviour therefore cuts across the risk to the protection of minors, as well as physical and mental well-being. Some providers noted that exposure to adult material may also contribute to the development of unhealthy behaviours or addictive consumption patterns amongst minors, with potential adverse effects on both mental and physical well-being. According to some providers, social comparison mechanisms may negatively affect minors' mental well-being by impacting their self-esteem via features such as likes providing "social rewards" that may reinforce patterns of compulsive use. Some CSOs mentioned the risk that features like endless feeds, autoplay and autoreplay of videos, the short length of videos, disruptive notifications, and highly-personalised recommender systems may exacerbate excessive screen time. Providers and CSOs also noted risks in relation to online marketplaces, specifically minors accessing products on online marketplaces intended solely for adults, but also compulsive shopping behaviour in online environments that encourage repetitive purchasing. Some CSOs identified systemic risks related to the protection of minors and public health, specifically noting that the omnipresence of commercial content may lead to compulsive consumption patterns and shopping addiction amongst adolescents.

EXPOSURE TO CONTENT THAT IS HARMFUL TO MINORS. This subcategory refers to content that may be lawful and not harmful for adults but is harmful for minors with potential adverse effects. For instance, graphic sexual content, the depiction or promotion of adult nudity or sexual activity,

including extended audio representations of sexual acts, the distribution of pornographic material, specifically extreme pornography, as well as sexually explicit language and persistent vulgarity have all been noted in risk assessment reports. Suicide, self-harm and eating disorder, as well as content relating to fitness and idealisation of body types are also risks in this category, as noted by providers. CSOs and providers noted that such content can be even more harmful if children are exposed to it, particularly where repeated exposure reinforces harmful norms or behaviours. Similarly, providers and CSOs mentioned that idealised body types and unrealistic standards of appearance can become problematic when consumed repeatedly. Minors are especially vulnerable when it comes to harmful "online challenges" on social media platforms, with severe risks for their mental and physical well-being. The dissemination of content related to harmful products and activities, such as alcohol or tobacco or money gambling on platforms, is also relevant. According to CSOs, minors might also have difficulty distinguishing between generative AI content and authentic content.

ACCESS TO UNLAWFUL CONTENT. The risk remains that minors access pornographic platforms that host age-inappropriate content by bypassing age-gating measures. Online marketplaces and social media platforms may also pose risks in the absence of safeguards such as lockout periods and session timeouts, as well as the sale or transfer of registered adult accounts to underage users, exposing minors to harmful content without appropriate safeguards. Access to gambling services may also lead to addictive behaviours.

CONTACT RISKS, EXPLOITATION AND ABUSE. Providers and CSOs noted several risks in relation to adult-minor interaction, exploitation and abuse. These include contact risks (such as grooming), sexual exploitation, solicitation, and coercion, sextortion and non-consensual sharing/threats regarding intimate images, CSAM production and dissemination, trafficking, sexualisation of ordinary images of minors (including using generative AI tools), cyberbullying and harassment by predators or peers, and psychological distress, trauma, and re-traumatisation. Some CSOs pointed out that the parasocial relationship between minors and content creators as a systemic risk, as commercial messages may be misperceived by minors as authentic personal recommendations.

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

Design and features: Providers and CSOs mentioned that features such as anonymous or pseudonymous profiles, direct messaging, or encrypted messaging may be misused by offenders to contact minors, facilitate grooming with a reduced risk of detection, although, at the same time, some CSOs mentioned that the possibility to express oneself anonymously online is an important safeguard to ensure the effectiveness of the right to freedom of expression. Some CSOs noted risks associated with the recommendations of contacts and

friends to minors which may be (adult) users they may not have known before, such as risks of grooming or cyberbullying. Furthermore, minors engaging with platforms that offer on-platform promotional activities or gaming-like interactions can increase addictive behaviour in minors. CSOs highlighted that platform design choices might be the most influential factor driving exposure towards illegal or age-inappropriate content. Providers and CSOs also noted that platform design features, such as infinite scrolling may contribute to extended use and difficulty disengaging from platform environments. Some CSOs reported that design features such as autoplay, infinite scroll and suggested queries can specifically make young users who have less inhibitory control vulnerable to compulsive or addiction-like behaviour on social media. Some CSOs also noted that risks may also arise from individual design features which are not problematic when used in isolation, but which may become harmful when functioning jointly with one another.

Recommender systems: Some CSOs and VLOPSEs noted that the design of recommender systems, such as optimising them for engagement, may lead to well-being risks linked to compulsive or addiction-like use or risks linked to being exposed predominantly and repeatedly to borderline harmful content, especially for minors.

AI systems: Some CSOs reported a potential systemic risk in the growing integration of AI tools into VLOPs used by children, enabling the creation of non-consensual sexualised images and facilitating exploitation, with such risks likely to increase as AI becomes more accessible and embedded in these platforms. Providers noted that emerging technologies such as AI may further facilitate the exploitation of minors or dissemination of harmful content by enabling or supporting exploitative practices. Some CSOs noted that AI tools, including agents and chatbots, embedded in VLOPs or VLOSEs may contribute to a variety of risks such as the dissemination of CSAM, misinformation and the increase of sexualised violence emanating as cyberbullying and cyber grooming. Researchers have also emphasised the growing risk associated with the increasing integration of AI tools into online platforms. Many of these tools are accessible by default rather than through selective use, and can, for example, enable the manipulation of minors' images. This increases the risk that such content could be exploited for financial extortion or coercion, particularly targeting children.

Content moderation systems: Some providers mentioned that user reporting mechanisms should be designed to be easily accessible to minors and age-appropriate, because if reporting tools are overly complex or not adapted to children's levels of comprehension, this may discourage or hinder reporting, thereby negatively affecting the effective protection of minors on the platform. Furthermore, if content is not moderated in a timely manner, this may affect children disproportionally, contributing to risks in relation to mental well-being. If content providers fail to accurately determine a user's age during moderation and appeals,

minors may gain access to experiences or content that are not age-appropriate, or may not receive protections specifically designed for younger users.

Examples of **observations by providers and CSOs** concerning systemic risks related to the **protection of minors**:

Google, 2025 DSA risk assessment, p.79: "*The systemic risk assessment reviewed several risks relating to minors' rights, such as behavioural addictions in minors, use of minors' data for ads targeting, and unnecessary or disproportionate limitations on minors' access to Search. We found the highest inherent risk to be the risk that minors under a defined minimum age access services that they should not be able to, and may be exposed to harmful, hateful, or age-inappropriate content or conduct"*.

Temu, in its 2025 DSA risk assessment report at p. 77 mentioned a "*risk of minors acquiring age-inappropriate products.* […] *Traders list a wide variety of products on Temu, including certain products that may be harmful to sell to minors*".

XVideos, 2025 DSA risk assessment report, p. 18: "*This category addresses the risks associated with underage individuals gaining unauthorized access to adult content, the potential creation or dissemination of exploitative material involving minors, and the failure of safety measures designed to protect them from harmful exposure. In the context of an adult content platform, ensuring the protection of minors becomes even more critical*".

TikTok, 2025 DSA risk assessment report, p. 60: "*The Platform could potentially be used for bullying behaviour or bad actors, such as child predators, groomers, cyberbullies, or scammers may attempt to use the Platform to discover or interact with Younger Users. Impacts on the mental wellbeing of Younger Users, which could, depending on the specific circumstances and/or choices of the individual, involve: (i) extended use of the Platform; (ii) exposure to Concentrated Content, which may be fine when viewed occasionally, but may be problematic if viewed repeatedly; (iii) social comparison; or (iv) risks arising from engagement with dangerous online trends or challenges (as well as related risks of physical harm)"*.

AliExpress, 2025 DSA risk assessment report, p. 43*: "The most critical risk vector, in this regard, is account creation (e.g., the risk that minors may misrepresent their age to create an account), thereby circumventing the Platform's controls and gaining unauthorised access to the service. Other risks include age-inappropriate content, where minors who have circumvented minimum age access requirements could be exposed to content or product listings that are compliant with platform policies but are still age-inappropriate (e.g., listings for adult products)"*.

KGI, a research institute dedicated to connecting independent research with technology policy and design, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"Problematic social media use is associated with a range of negative outcomes for minors, including risks related to social comparison, body image, dissatisfaction, and disordered eating, displacement of healthy behaviours, and broader feelings of sadness, anxiety, depression, and stress"*.

Save the Children Denmark, a CSO dedicated to protecting children's rights, submission to the invitation for contributions from the European Board for Digital Services and the European Commission: *"A potential systemic risk that may currently be overlooked is the increasing integration of AI tools into online platforms used by children and young people. These AI functionalities can enable image manipulation, including the creation of nonconsensual intimate or sexualised images of minors. Such manipulated content can subsequently be used for financial extortion or coercion targeting children. This risk deserves particular attention because AI tools are no longer only accessed deliberately. They are now embedded by default within widely used online platforms, meaning that children and young people may be exposed to advanced AI capabilities, even when they do not actively seek them out"*.

3.4.4. Physical and mental well-being

Systemic risks to physical and mental well-being are prominent, to varying degrees, on all VLOPs and VLOSEs. Physical and mental well-being also cuts across risk categories, in particular risks to minors and risks of GBV. Providers of VLOPs and VLOSEs such as social media, pornographic platforms and search engines are the most relevant with regard to risks related to physical and mental well-being.

PHYSICAL WELL-BEING. Risks to physical well-being may stem from unsafe or inadequately described products on online marketplaces, physical violence facilitated or promoted via online platforms, including intimate partner violence, as well as physical danger from deceptive job postings or unsafe contact facilitation. Self-harm, suicide, and eating disorders, including from content that promotes, glorifies, or normalises such behaviour has also been observed by providers and according to experts is most prevalent on social media platforms, despite it not affecting the general population. Finally, harmful effects of content promoting unrealistic beauty standards, extreme fitness trends, or unhealthy body ideals have been noted by providers, while CSOs noted that generative AI tools embedded in VLOPs or VLOSEs may exacerbate this risk. Excessive screen time has been associated with potential physical well-being risks such as myopia and strain on eyesight by researchers.

MENTAL WELL-BEING. Providers noted the risk of compulsive/excessive platform use and its effects on relationships, productivity, mental stability, and attention span. As covered in the previous

sections, this compulsive use risk is particularly pertinent on social media platforms, but it also relates to addiction to pornographic content and compulsive shopping behaviour with financial and psychological consequences. These risks are particularly acute for minors, as is the stress, anxiety, and reduced self-worth from unrealistic expectations regarding sexual performance or physical appearance. Trauma and re-traumatisation from content depicting sexual abuse or severe violence, including for victims of exploitation alongside fear, anxiety, and panic from exposure to highly graphic content (e.g. extreme pornography, terrorist content) was also noted by providers as a source of risk to mental well-being. Prolonged exposure to harmful content, targeted harassment, cyberbullying, insults as well as illegal hate speech (directed at the user or directed to other users witnessed by the user) can lead to risks of anxiety related to a high exposure to news content on social media, for example in relation to armed conflicts or environmental issues.

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

Design and features: Providers and CSOs noted that infinite scrolling, continuous engagement, deep browsing pathways, repeated exposure to personalised content, reward mechanisms, time-limited promotions, and interactive games facilitating compulsive purchasing are all factors that can have a negative impact on mental well-being. Accordingly, CSOs observed that the ways in which content is displayed and ordered can have a significant impact on the length of time young people use platforms for and can play a role in addiction-like behaviour amongst younger users. Some providers acknowledged this by stressing that there was a risk that parts of the design of a service could be addictive or manipulative.

Monetisation policies and their enforcement: Some CSOs stressed the importance of design choices and monetisation policies and their role in the emergence of systemic risks for example related to the excessive and compulsive use of a service which business model relies on the maximisation of users' engagement including their time spent on the service.

Recommender systems: Through recommender systems, users can encounter content that is harmful to their well-being, or that promotes harmful conduct. Engagement-based recommender systems could further create feedback loops that lead to repeated exposure to, for instance, unrealistic beauty standards, thereby negatively affecting users' mental well-being over time. Crucially, even in the absence of harmful content, engagement-based recommender systems may lead to addiction-like behaviour.

Examples of **observations by providers and CSOs** concerning systemic risks related to **physical and mental well-being**:

Zalando, 2025 DSA risk assessment report, p. 18: *"While all* [Zalando's] *platform services and functionalities are primarily designed for fashion-related inspiration and expression, they must be assessed for potential unintended negative impacts stemming from the design interface that could be perceived as addictive or manipulative. Algorithmic systems are powered by user data, which is continually refined through increased user engagement. This dynamic creates a feedback loop: the more users interact with the platform, the more accurately the system can deliver personalised and relevant content. This can lead to repeated exposure to certain types of imagery, beauty standards or style ideals, that can have a negative impact on users' mental well-being over time"*.

Instagram, 2025 DSA risk assessment report, p. 88-89: *"The* [Suicide, Self-Injury and Eating Disorders] *Problem Area relates to the risk of Instagram being used to promote, speak positively, encourage, coordinate, or provide instructions for SSIED, potentially including ads that could impact public health. This also potentially includes: depictions of graphic self-injury, suicide attempts, death by suicide, instructions for extreme weight loss, content admitting to extreme weight loss behaviour when shared together with terms associated with eating disorders, depictions of body parts with terms associated with eating disorders, and content mocking victims or survivors of suicide, self-injury, and disordered eating"*.

Shein, 2025 DSA risk assessment report, p. 61: *"This risk could apply on the Marketplace through the exposure of users to addictive design features that incentivise users to spend extended periods of time on the Marketplace, e.g. unlimited scrolling and spending money compulsively"*.

Stripchat, 2024 DSA risk assessment report, p. 41: *"Users, visitors, models or studios using Stripchat for direct or indirect dissemination of materials, promoting, depicting, describing or referring in a positive context to extreme pornography potentially detrimental to individuals' physical and mental well-being"*.

XVideos, 2025 DSA risk assessment report, p. 21: *"Risk scenarios illustrate the potential harm within this category. Addiction concerns (PH_1) highlight the risks associated with compulsive content consumption, which can interfere with daily life, relationships, and psychological well-being, although researchers have declined to classify excessive or compulsive pornography use as an addictive behaviour"*.

Chapter 4

Practices to mitigate systemic risks

4. Practices to mitigate systemic risks

Article 35(2) DSA requires that the Board report include "best practices" for providers of VLOPs and VLOSEs to mitigate the systemic risks identified pursuant to Article 34.

As with previous reporting cycles, however, because the DSA is still at an early stage of its implementation, including of Articles 34 and 35, this edition of the Article 35(2) DSA report does not yet single out any mitigation practices presented in this Chapter as "best" or even "good" practice across the board. Instead, the Sections that follow map and organise the range of mitigation approaches currently observed across different categories of services, drawing on providers' reports under Article 42(4) DSA, civil society and academic analyses, and other available sources listed in the Annex to this report.

As regards the publication of the annual risk assessment reports by VLOPs and VLOSEs, which detail systemic risks and mitigation measures, the fact that a mitigation measure is widely adopted is not necessarily to be interpreted as an indication of its effectiveness, suitability, or alignment with best practices. The providers' choices in deploying certain mitigation measures are shaped by a range of factors, including scalability, cost, operational complexity, competitive dynamics, and business incentives. For example, a mitigation measure may be widely adopted because it is easier or cheaper to implement, rather than because it delivers the best outcomes for users. Likewise, the fact that a mitigation measure is mentioned does not mean that it is necessarily applied in practice in a way that actually mitigates risks or in a way that would ensure compliance with Article 35 DSA. For example, it is not because screen time management tools are mentioned as having been implemented by some providers that such time management tools are actually effective at mitigating certain risks.

The categories of services outlined in Sections 4.2 to 4.4 (social media, online marketplaces, pornographic platforms and search engines) may overlap. For example, a social media may have integrated marketplaces functionalities; in this case, the mitigation measures mentioned in Section 4.3 below would still be relevant to it although Section 4.2 is the one mainly focusing on social media. The same goes also for example for marketplaces or pornographic platforms that integrate social features.

As in last year's edition, and as stated in Chapter 1, nothing in this report should be interpreted as guidance for 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. Likewise, this Chapter does not elaborate on measures

presented by providers as mitigation measures but that are in reality undertaken as part of compliance with other acts of Union law.

Future editions of this report will draw on the European Commission's enforcement actions and evidence gathered by stakeholders to identify best practices for mitigating systemic risks. In the meantime, to keep the report concise, mitigation measures should be read cumulatively: each edition adds new measures to those outlined in previous years. As a result, some measures included last year, while still relevant, may not be repeated in this edition in order to make room for new ones.

To enable providers of VLOPs and VLOSEs and CSOs to best identify reasonable, proportionate and effective mitigation measures, recital 90 DSA encourages providers of VLOPs and VLOSEs to ensure a meaningful involvement of representatives of users, affected groups, CSOs and researchers.

Engagement with stakeholders in the assessment of risks and their mitigation. Recital 90 DSA highlights the importance for providers of VLOPs and VLOSEs to engage with outside stakeholders, including CSOs, to inform their risk assessment and mitigation process, so as to provide a safe online environment for users. Providers mentioned engaging with a variety of stakeholders, such as CSOs, think tanks, research communities, independent fact checkers, law enforcement authorities. Interactions with external stakeholders which have been mentioned by providers and CSOs took the form of one-off consultations, long-term partnerships, roundtable discussions, focus groups (especially with vulnerable groups), research collaborations with experts, Q&A sessions, briefings and working groups. At the same time, it is not because some providers mentioned engaging with CSOs and other stakeholders that they would have necessarily done so in a meaningful way in the spirit of recital 90 DSA.

Some CSOs observed that providers' engagement with external stakeholders for risk assessments should increase and deepen, and that feedback should be incorporated in meaningful ways. In particular, some CSOs mentioned the importance of publishing metrics for risk assessments such as results from A/B tests of features that have been associated with systemic risks (e.g. recommender systems, interface design choices) to better involve stakeholders into the identification and mitigation of systemic risks. Likewise, some CSOs mentioned the importance of collaborating with CSOs, trusted flaggers, researchers and affected communities in the development of risk assessments and mitigation measures, in the spirit of recital 90 DSA. Article 35(1)(g) DSA refers to cooperation with trusted flaggers and the implementation of decisions of Out-of-court Dispute Settlement Bodies as possible sources of mitigation measures. To ensure clarity on how this mechanism operates, the Commission has been developing guidelines on trusted flaggers. In May 2026, the Commission has launched a

targeted consultation on draft guidelines on trusted flaggers under the DSA, giving relevant stakeholders the opportunity to share their insights[17].

Data access mechanisms and live public data monitoring tools for CSOs and researchers are key to enable effective third-party scrutiny and to contribute to the risk mitigation cycle that providers of VLOPs and VLOSEs carry out yearly. Access to reliable data on the services enables CSOs and researchers to effectively support the early detection of systemic risks and to better understand the effectiveness of the mitigation measures providers put in place. As such, access and scrutiny mechanisms are a key component of providers' risk mitigation measures, making them more robust. CSOs' and researchers' cooperation becomes even more crucial and time-sensitive during special periods, such as crises or elections, where robust scrutiny is time-sensitive. For this reason, the Commission guidelines on electoral processes recommend *"stable and reliable data access for third party scrutiny* [as] *of utmost importance during electoral periods to ensure transparency, advance insights and to contribute to the further development of risk mitigation measures around elections".*

RELATED CODES OF CONDUCT AND GUIDELINES.

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) 2022/206518, 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) 2022/206519, as well as the Code of Conduct on Disinformation[20] and the revised Code of Conduct on countering illegal hate speech online[21].

[17] Draft Communication from the Commission – Guidelines on the trusted flagger mechanism under Article 22 of Regulation (EU) 2022/20265, available at the following link: https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-trusted-flaggers. The deadline for submitting input was extended to 10 July 2026.

[18] 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.

[19] 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/HTML/?uri=CELEX%3A52020DC0790.

[20] 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.

[21] 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.

However, this report does not elaborate or provide an evaluation of the uptake of such measures by providers.

On 13 February 2025, the Commission and the European Board for Digital Services endorsed the official integration of the voluntary Code of Practice on Disinformation into the framework of the DSA as a Code of Conduct. In the Commission Opinion on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 DSA, the Commission concluded that *"the Code of Practice on Disinformation contributes to the proper application of the Regulation (EU) 2022/2065".*

Moreover, in the same document the Commission stated: *"As set out in the detailed assessment, the Code of Practice on Disinformation is a worldwide pioneering robust set of Commitments and detailed Measures that taken together constitute a strong set of mitigation measures. As a result of its integration in the co-regulatory framework of Regulation (EU) 2022/2065, adherence and compliance with it by a provider of VLOPs or VLOSEs may be considered as an appropriate risk mitigation measure under Article 35 of Regulation (EU) 2022/2065. In practice, the Code will become a significant and meaningful benchmark for determining compliance with the Regulation (EU) 2022/2065 for those providers of VLOPs and VLOSEs that adhere to and comply with its Commitments".*

Similarly, the European Board for Digital Services in its Conclusions on the recognition of the Code of Practice on Disinformation as a code of conduct pursuant to Article 45 DSA stated: *"The Board acknowledges that the Code may therefore be taken into account in the context of the compliance assessments pursuant to Articles 34 and 35 of the DSA, following its conversion into a code of conduct under Article 45 of the DSA. The Code can notably — subject to its implementation in practice — become a significant benchmark for DSA compliance regarding mitigating systemic risks related to disinformation. The higher the level of compliance with the Code, the more positive the impact on the assessment of risk mitigation under Article 35 of the DSA".*

In that view, and as set out in the European Democracy Shield: *"*[t]*he Commission will assess the levels of commitment of individual signatories of the Code and their implementation"*, and *"*[i]*f necessary, the Commission will hold regulatory dialogues, under the DSA with signatories of the Code and decide about other appropriate follow-up actions"*. Such dialogues might also support the identification of suitable practices and help the Commission to identify best practices for providers of VLOPs and VLOSEs to mitigate systemic risks related to disinformation.

4.1. Risk mitigation measures relevant to all providers

4.1.1. Terms and conditions and their enforcement

Under their obligations resulting from Articles 14 and 35(1)(a) DSA, most providers mentioned not only having general terms and conditions but also specific policies and community guidelines for specific types of content. For example, some app stores providers mentioned dedicated developer policies to determine what apps developers can and cannot provide, including specific guidelines for apps that rely on user-generated content. Some social media providers mentioned having adopted hate speech policies, manipulated media policies, or child safety policies. In the same vein, some online marketplaces mentioned policies to prohibit the sale or promotion of certain products, e.g. via dangerous products policies. Some CSOs mentioned the importance of including prohibiting uploading intimate images without consent, and limiting content promoting extreme misogyny and GBV.

For users that repeatedly circumvent or breach policies, many providers deploy measures such as the rejection, removal, suspension of apps, contents and accounts, limiting the visibility of contents and accounts in certain geographical areas, and account termination. For example, some providers of online marketplaces have measures in place to ensure that sellers who repeatedly breach terms and conditions cannot reopen their store or open any new stores, as well as having pre-deployment checks and pre-listing interception tools. Some CSOs stated that the moderation of scam networks and accounts, including inauthentic advertisers, could include evaluating behavioural patterns across a users' full use history, not only individual advertisements or pieces of content. Furthermore, some providers and CSOs highlighted specific sanctions for creators who fail to disclose commercial partnerships, as well as the demonetisation of fact-checked content where that check concluded that the content was not factually correct. Some CSOs also mentioned using account-level enforcement actions instead of content-level moderations for users posting harmful content or engaging in coordinated inauthentic behaviour.

4.1.2. Content moderation and risk detection

With regard to content moderation and risk detection, most providers of VLOPs and VLOSEs mentioned using both automated and human means, as well as both pro-active and re-active approaches.

AUTOMATED/HUMAN CONTENT MODERATION. Regarding the automated/human interactions for content moderation, some providers and CSOs mentioned for example automated tools to analyse text, images or videos, and behavioural signals to flag suspicious content or products at scale, with escalations to trained human reviewers when more nuanced judgment is needed. Some providers explained having created processes where human reviewers' decisions continuously retrain classifiers to improve detection models over time. Some providers also

mentioned establishing specific human task forces for specific risks or during specific periods (e.g. intellectual property, electoral processes). Some providers have also reported implementing quality assurance through performance monitoring, model testing, and regular updates to policies and procedures, in an attempt to enhance consistency and reduce bias in enforcement. Some CSOs suggested testing content moderation results against the results of tests using gold standard labelled data. Some providers mentioned trainings on risk detection for their content moderation staff, for example focusing on online trust and safety in general, as well as on specific risks and specific legal requirements (including DSA-specific trainings) and local cultural specificities. Likewise, some CSOs mentioned the importance of dedicated trainings for certain risks, such as GBV. Some CSOs mentioned the importance of having trained moderators with linguistic and cultural competence in relevant regional languages and dialects to accurately assess contextual meaning, coded language, and culturally specific hate narratives.

PROACTIVE AND REACTIVE CONTENT MODERATION. Regarding the pro-active/re-active approaches to content moderation, some providers mentioned tools to detect GBV or CSAM material before it becomes searchable, for example by using hash-matching technologies before or during indexing and then reporting that illegal content to competent authorities in accordance with legal obligations. Hash-matching has been mentioned by providers and CSOs in different context such as terrorism, GBV or CSAM. Some providers also mentioned similar safeguards to prevent illegal or policy-violating content from being included in training data for algorithmic and AI systems. Providers also reported specific user-facing reporting routes that allow recipients of the service (or affected persons) specifically to flag non-consensual material for review, supporting notice-and-action and victim reporting pathways. Additional safeguards such as specialised moderation queues have also been outlined by providers. Some providers mentioned collaborations with online risk intelligence organisations and cross-platform data sharing to detect coordinated inauthentic behaviour.

4.1.3. Safety by design

Providers of VLOPs and VLOSEs reported using various design features to mitigate systemic risks. For example, some providers mentioned using protective default settings for minors such as disabling autoplay features by default, implementing content blurring, warning labels and trigger warnings for graphic content. Some providers mentioned designing their services not to allow infinite scrolling. Some CSOs mentioned the importance of monetisation policies that do not incentivise providers to maximise user engagement and time spent. Some CSOs highlighted the importance of integrating design elements that foster inclusive and less polarising discussions to improve the civility of interactions amongst users. Some CSOs mentioned policies and design elements that promote and encourage digital inclusion, such as simple language options, dictation abilities, readability enhancements and auto-generated captions on videos, to help mitigate risks of marginalising certain voices or groups.

4.1.4. User empowerment

With regard to recommender systems, some providers and CSOs mentioned tools permitting users to set their recommendations preferences, for example to allow more or less of specific types of content. Some CSOs mentioned settings for users to reset their recommender systems' profiles, or to disable recommender systems altogether (to rely instead on chronological feeds). Likewise, some providers, as well as CSOs, mentioned the importance of embedding recommender systems with prioritisation objectives other than engagement/watch-time in order to reduce risks associated with the promotion of sensationalism and outrage, but also other risks, for example related to addiction-like behaviour on social media. Some providers and CSOs mentioned mitigation measures against risks of excessive use in the form of self-control mechanisms through interface design nudges to limit usage, as well as time management and time limitation tools.

4.1.5. User awareness

Providers mentioned having implemented measures to raise users' awareness about certain matters. These included for instance, crisis support tools, such as bullying and harassment centres, suicide prevention resources, emotional and mental health hubs, and family digital wellness guides, alongside general help centres. Some providers specifically mentioned help pages on how to avoid scams. Some providers have reported the implementation of political awareness campaigns and training, such as deceptive AI and elections training. Some providers of online marketplaces have also reported specific education programmes for sellers and customers, with specialised courses on key compliance or risk issues (e.g. IP, data protection). In some instances, some providers reported having implemented awareness notifications with real time guidance in the user journey (e.g. alerts when counterfeits are searched for, interstitials with warnings for searches on topics like suicide). Some providers mentioned features to explain users why specific advertisements are showed to them.

4.1.6. Out-of-court Dispute Settlement

Some CSOs and Out-of-Court Dispute Settlement Bodies (ODSBs) noted that implementing ODSBs decisions can contribute to mitigating the risks of proliferating illegal hate speech, terrorist content and gender-based violence giving an additional recourse for users to contest content moderation decisions by VLOPSEs regarding potentially violative content, including in cases where the internal complaint handling system has not led to content removal. At the same time, however, implementing ODSB decisions can also serve as an effective mitigation measure against risks to fundamental rights, in particular freedom of expression and non-discrimination, as it allows users to seek redress, potentially leading to content or accounts being reinstated.

4.2. Risk mitigation measures particularly relevant to social media platforms

Besides the risk mitigation measures relevant for all providers described above in Section 4.1, this section presents risk mitigation measures particularly relevant to social media platforms.

MITIGATION MEASURES IN RELATION TO INFORMATION INTEGRITY AND CONTENT AUTHENTICITY. Some providers and CSOs mentioned mitigating measures such as "geo-blocking" harmful content to limit the reach of that content, as well as community notes to enable users to provide context to content and warn other users about misleading information or unsafe links embedded in that content. Some CSOs mentioned combining fact-checking programmes and community notes as a mitigation measure against disinformation risks. Some providers reported an in-app page to connect users with reliable information about voting. Some providers mentioned having joined initiatives such as the Coalition for Content Provenance and Authenticity ("C2PA"), an open technical standard and content provenance solution to provide information in a piece of content's metadata about its origins and whether generative AI was used to create or edit it.

Some providers mentioned having policies to prohibit the use of generative AI to show the likeness of natural persons without their permission or prohibit violative content at prompt-level in AI chatbots. Some providers started programmes to allow famous individuals to opt-in to receive "celeb bait protection" so that their likeness may not be used in generative AI content on their services. Some CSOs mentioned potential mitigation measures with regard to account authenticity and civic discourse risks such as specific verification badges for political accounts in the EU or limiting the possibility to create inauthentic fan accounts for political figures. Some providers mentioned having introduced content labels and watermarks for AI-generated content. Some providers mentioned conducting AI red teaming to simulate attackers who might target AI systems and assess AI systems for systemic risks and areas of improvement. Some CSOs mentioned the conduct of election-specific reviews of the enforcement of certain policies around civic discourse, risk detection and content moderation.

Mitigation measures in relation to the **protection of minors**:

Some providers and CSOs mentioned the importance of enforcing a minimum age requirement and age gates, facilitating removal of accounts belonging to users below the minimum age stipulated in the provider's terms and conditions or where a minimum age to access certain content is provided for by law, and providing tools to manage who can follow minors' accounts, as well as requiring a parent or guardian's approval for certain key changes to account settings. Some CSOs highlighted the possibility of authenticating users' profiles with national digital IDs in order to verify their age. Some providers mentioned the existence of settings allowing parents and guardians to establish a supervised experience for minors, for example allowing parents and guardians to set parameters on what kinds of content minors can see, screen time limits etc.

Some CSOs mentioned the possibility to turn off infinite scrolls for minors with non-circumventable daily time limits or limits on the number of pieces of content that may be watched. Some providers mentioned setting higher account safety settings by default for minors (e.g. by setting some features, such as location, to private), avoiding techniques that encourage teenagers to share more data and offering closed spaces for teens to express themselves without public likes and comments. Some providers reported having default settings for logged-out users not permitting to view sensitive media and displaying only advertisements which are tagged as "family safe". Some providers highlighted the rollout of teen accounts (users in the age range of 13-17) with additional protection features.

Some providers require, by default, that users need to accept bi-directional friend requests or have each other in their contact book to start communicating. Some providers mentioned settings to keep a friends' list private, or turning all users' precise location sharing off by default. Some providers reported only allowing users with an older teenage account (16-17) or an adult account (18+) to have a public profile and to share certain content publicly. Some providers mentioned having raised the minimum age for livestreaming from 13 to 16 years old.

Some providers mentioned the detection and removal of CSAM through hashing and automated matching of content against known CSAM-imagery. In case of signals of potential child abuse, some providers mentioned reviewing the relevant direct messages in respect of the applicable law. Some CSOs mentioned the importance of strong optical character recognition (OCR) and image-recognition technology to enhance the reliability of content moderation, in particular to detect illegal hate speech and incitement risks on social media.

4.3. Risk mitigation measures particularly relevant to online marketplaces

Besides the risk mitigation measures relevant for all providers described above in Section 4.1, this section presents risk mitigation measures particularly relevant to online marketplaces.

MITIGATION MEASURES IN RELATION TO USER/TRADERS VERIFICATION AND CONTENT AUTHENTICITY. Some providers require verification of all buyers and sellers, including account level verification through mandatory product compliance certificates for sellers, and proof of seller registration with a government authority. Some providers have created a mechanism for in-person verification of traders. Some providers reported having established a pre-screening mechanism for affiliate programme participants' declared channels. Some providers mentioned using verification mechanisms for traders and listings to verify their existence and location, and use fraud detection including automated tools to detect fake listings, marketing fraud and evolving fraud patterns. Some providers, to protect users from fake reviews and ratings, use automated fake review and rating detection tools, conduct proactive review of third-party sites (e.g. social media sites where transactions underlying fake reviews may happen) and collaborate with

other providers to take down bad actors. Some providers reported having adopted detection tools to detect fraudulent business information, harmful keyword matching, and vetting and monitoring mechanisms for merchants and listings. Some providers reported mandatory information disclosure for traders, dedicated onboarding and the sharing upload of product compliance information.

MITIGATION MEASURES IN RELATION TO ILLEGAL OR NON-COMPLIANT PRODUCTS. Some providers mentioned the use of EU-based third parties to monitor and sample live listings to limit large-scale and repeated uploads to prevent bad actors from re-listing illegal/harmful products. Some providers reported procedures to re-call non-compliant products. Some providers mentioned having created frameworks to identify and address worst offenders. Some providers mentioned enforcing a retention of commissions for affiliate programme participants listing illegal content. Some providers mentioned automated tools to identify deliberate mis-categorisation of prohibited goods. Some providers mentioned conducting daily spot checks on physical products through partnerships with third parties, controls for document compliance and expiry, product recall procedures and correcting misplaced product categories.

MITIGATION MEASURES IN RELATION TO VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS. Most providers mentioned having specific IP rights infringement policies and IP rights violation detection tools. Some providers mentioned having content and brand guidelines to prohibit offensive, illegal or inappropriate products and content. Some providers mentioned having in place intellectual property checks both pre-listing (where sellers have to submit proof of rights before listing a product) and post-listing (through automated means). Some providers mentioned having dedicated counterfeit crime units to increase civil litigation efforts and criminal referrals in partnership with brands and law enforcement organisations. Several providers mentioned having established dedicated tools to empower rightsholders to protect their brands on their platform. Some providers also mentioned directly allowing brands and rightsholders to remove counterfeit products themselves.

MITIGATION MEASURES IN RELATION TO SOCIAL FEATURES IN ONLINE MARKETPLACES. Some providers reported detecting and removing third party links redirecting users off-platforms. This includes also specific measures against hidden links that may be spread through affiliate programmes. On the other hand, in order to limit interaction risks, some providers simply do not allow communications between users. Some providers, to limit risks from affiliation and influencers, created dedicated affiliate and influencer policies and conduct manual reviews of published influencer content. Some providers also mentioned reviewing livestreaming announcements and monitoring livestreams. Some providers mentioned plans to launch enhanced anti-discrimination contractual requirements for their traders.

MITIGATION MEASURES IN RELATION TO APPLICATION STORES. Some providers mentioned having created developer onboarding and verification processes, as well as training and guidance

material. Some providers require app developers to provide links to any regulatory certifications they may have received. Providers mentioned both automated and manual app-review and verification systems. For certain health-related apps, some providers mentioned having created a requirement for developers to remind users to check with a doctor in addition to using the app and before making medical decisions. Some providers created badges for "verified" VPN apps for security and safety reasons, noting the elevated risk for those types of apps in particular. With regard to educational apps, in particular for children under 13, some providers mentioned specific quality reviews to collect ratings from teachers, minors' education specialists, and media specialists. Some providers developed guidelines for users when writing reviews or ratings.

Mitigation measures in relation to the **protection of minors:**

Certain providers do not allow minors on their service. Some providers, to prevent minors from using their services, mentioned using specific measures such as requiring that an account can only be opened with a credit card, which in some Member States may only be issued to persons above 18. Some providers reported preventing the dissemination of age-inappropriate content to minors, such as adult advertisements for minors, others mentioned not allowing the recommendation or the advertising of adult toys. Some providers mentioned using warning labels on products (e.g. for toys), blurring adult-only product lists in search results and having pop-up windows requiring users to confirm that they are over 18 to unblur the images, and limiting interactive activities or coupons to adults only. Some providers mentioned applying the highest prioritisation for the detection of nudity and CSAM. Some providers reported having rolled out age ratings and dedicated categories of apps for kids. Some providers mentioned parental control tools so that parents and guardians can for example share only an age range rather than the actual age of their children, set screen time limits or require approval for app downloads. Relatedly, some providers mentioned features to permit developers to block minors from downloading or purchasing an app, continuing a subscription, or making new purchases on an app that is already installed, as well as to permit their apps to reach age-appropriate audiences. With regard to educational apps, in particular for children under 13, some providers mentioned specific quality reviews to collect ratings from teachers, minors' education specialists, and media specialists.

4.4. Risk mitigation measures particularly relevant to pornographic platforms

Besides the risk mitigation measures relevant for all providers described above in Section 4.1, this section presents risk mitigation measures particularly relevant to pornographic platforms.

Concerning the verification of content creators, some providers mentioned requiring that performers of professional studios as well as user uploaders verify their identity and the identity

of third parties depicted in the uploaded content (e.g. through the KYC onboarding process for content partners), verify their age, and verify their consent (e.g. by signing a consent agreement, consent which they may withdraw at any time). Some providers mentioned the deployment of informational and training resources to prevent sex trafficking risks. Some CSO mentioned the possibility to present contextual warnings that inform users posting content that it is a criminal offence to upload material without the consent of those depicted. Some providers mentioned measures to prevent the creation and sharing of deepfakes content portraying individuals. Some providers reported restricting functions such as messaging to registered users only. Some providers mentioned having created resources for users (and content creators) such as blogposts, newsletters, guidelines, campaigns, sexual wellness information pages on their websites with educational material on sexual health and pointing to related third party resources. Some providers mentioned prohibiting content downloads, or de-listing URLs from search results.

Mitigation measures in relation to the **protection of minors**:

Most providers put an emphasis in their reporting on the mitigation of risks related to the protection of minors, including age assurance systems, content warnings, page blurring, and using RTA ("Restricted To Adults") labels to enable parental filtering and control tools. Some providers mentioned tools to detect possible minors or banned users on their service. Regarding CSAM, some providers mentioned automated detection tools (e.g. PhotoDNA), CSAM deterrence messages and chatbot support for users searching for CSAM, as well as various support tools for users, such as an anonymous CSAM reporting tool and a CSAM helpline.

4.5. Risk mitigation measures particularly relevant to online search engines

Besides the risk mitigation measures relevant for all providers described above in Section 4.1, this section presents risk mitigation measures particularly relevant to online search engines.

Some providers mentioned minimising exposure through ranking and filtering instead of broadly removing search results. Some providers mentioned using human search quality raters to test and improve the search algorithm; in parallel, they include measures to prevent the dissemination of ads that potentially benefit from disasters, public health emergencies, acts of terrorism, or similar critical events. Some providers reported prioritising information from official channels when users search for election-related terms. Some providers, for search queries related to self-harm, eating disorder, suicide or similar high-risk sensitive topics, redirect users to reach out to family, friends and mental health professionals, and provide high authority content. With regard to non-consensual sharing of intimate images and sexualised deepfakes, some providers mentioned having put in place a removal process for users to more easily request removal of these types of content from search results, as well as information

literacy training programmes to educate users on how to examine and analyse content they find online. Some providers, addressing safe search generally and AI-generated content such as deepfakes specifically, mentioned restricting visual search features so that they cannot match private individuals' faces.

Chapter 5

Outlook

5. Outlook

This is the second 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 actions taken by the Commission and the DSCs with regard to VLOPs and VLOSEs providers, such as the non-compliance decision adopted against Temu on 28 May 2026 (C(2026) 3646 final), in which the Commission concluded that the provider of Temu failed to diligently identify, analyse, and assess the systemic risks of illegal products being offered on its platform and the resulting harm to consumers in the European Union (Article 34(1) and (2) DSA). This was the first non-compliance decision adopted under the risk assessment framework of the DSA.

Overall, 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. Insights from the monitoring of the Codes of Conduct, notably the Code of Conduct on Disinformation as well as the Code of Conduct on Hate Speech will also inform future editions. Developments in the implementation and enforcement of other DSA provisions such as the data access mechanisms of Article 40 DSA, and notably the research outputs resulting from such data access, will further 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, and so will future non-compliance decisions adopted on the basis of Articles 34 and 35 DSA.

Annex

Resources and studies from independent experts, civil society organisations and other stakeholders

Annex: Resources and studies from independent experts, civil society organisations and other stakeholders

The lists below contain public resources and studies from independent experts and CSOs as well as input from CSOs, trusted flaggers, ODSBs 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 March 2026:

- Appeals Centre Europe (ACE)
- Agence France Presse (AFP)
- Algorithm Watch
- Bee Secure
- Belgian Institute for the Equality of Women and Men
- Bundersverband Frauenberatungsstellen und Frauennotrufe (bff)
- Centre for Democracy and Technology (CDT)
- Child Helpline International
- Foundation Diaspora in Action for Human Rights and Democracy (DAHRD)
- Democracy Reporting International (DRI)
- Digitálna inteligencia (digiQ)
- Echipa Funky Citizens
- European Centre for Non-profit Law (ECNL)
- European Fact-Checking Standards Network (EFCSN)
- European Partnership for Democracy (EPD)
- Federation LGBTI+
- International Network Against Cyber Hate (INACH)
- Jugend Schutz
- Knight-Georgetown Institute (KGI)
- Fundación Maldita.es
- Mimikama
- "NEVER AGAIN" Association
- None Of Your Business (NOYB)
- Online Rizika
- Panoptykon
- Point de Contact
- Reset Tech
- Save the Children Denmark
- Smex
- SOS Racisme

- Stiftung Digitale Chancen
- What to Fix
- WomensAid

LIST OF OTHER SOURCES FROM INDEPENDENT RESEARCHERS AND CSOS WHICH WERE CONSIDERED FOR INPUT FOR THIS REPORT OF THE BOARD AND THE COMMISSION (IN CHRONOLOGICAL ORDER):

Authors(s)	Title	Date	Links
Jóźwiak	The DSA's Systemic Risk Framework: Taking Stock and Looking Ahead	05/2025	https://dsa-observatory.eu/2025/05/27/the-dsas-systemic-risk-framework-taking-stock-and-looking-ahead/
Cooper & Chapman (KGI)	Systemic Risk Assessment under the Digital Services Act	05/2025	https://kgi.georgetown.edu/research-and-commentary/systemic-risk-assessment-under-the-digital-services-act/
Del Campo et al. (Cele)	Reclaiming Human Rights for Platform Governance: Proposals for Restoring Their Centrality in the Era of Risks	05/2025	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5265938
Reich (Liberties)	Undue Influence(rs): How Platforms Must Step Up under the DSA to Protect Democracies Policy Recommendations for VLOPs, VLOSEs, and The European Commission	05/2025	https://www.liberties.eu/f/khrynp
Matlach & Drath (Institute for Strategic Dialogue)	The 'Cost of Doing Politics'? Gendered Abuse and Digital Platforms' Role in Undermining Democracy	05/2025	https://www.isdglobal.org/publication/the-cost-of-doing-politics-gendered-abuse-and-digital-platforms-role-in-undermining-democracy/
5 Rights et al.	Joint EU letter calls for robust risk assessment for children's rights under the DSA	06/2025	https://5rightsfoundation.com/resource/joint-eu-letter-calls-for-robust-risk-assessment-for-childrens-rights-under-the-dsa/
Holznagel	Shortcomings of the first DSA Audits — and how to do better	06/2025	https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/
Holznagel	DSA - Risk Assessment & Mitigation: 3 Thoughts on the first Reportings	06/2025	https://www.otto-schmidt.de/blog/it-recht-blog/dsa-risk-assessment-mitigation-3-thoughts-on-the-first-reportings-ITBLOG0007909.html
Holznagel	Die Regulierung von Empfehlungssystemen im DSA — Status Quo und Herausforderungen.	06/2025	https://www.degruyterbrill.com/document/doi/10.9785/cr-2025-410514/html

AI Forensics	AI Generated Algorithmic Virality	07/2025	https://aiforensics.org/work/gen-ai-slop
Eurochild	From advocacy to action: how Eurochild is shaping child protection under the DSA	07/2025	https://eurochild.org/news/from-advocacy-to-action-how-eurochild-is-shaping-child-protection-under-the-dsa/
GNI & DTSP	European Rights & Risks: Stakeholder Engagement Forum 2025 EVENT SUMMARY	07/2025	https://globalnetworkinitiative.org/new-report-2025-european-rights-risks-stakeholder-engagement-forum/
Sekwenz et al.	From Reports to Reality: Testing Consistency in Instagram's Digital Services Act Compliance Data	07/2025	https://arxiv.org/html/2507.01787v1
Palubo & Ducuing	The Blurring of the Public-Private Dichotomy in Risk-Based EU Digital Regulation: Challenges for the Rule of Law	08/2025	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5395729
AI Forensics	YouTube's Safety Features Lost in Translation	08/2025	https://aiforensics.org/work/youTube-safety-features
Fabbri & Boratto	Auditing Recommender Systems for User Empowerment in Very Large Online Platforms under the Digital Services Act	09/2025	https://dl.acm.org/doi/10.1145/3705328.3748074
AlgorithmWatch	Happy Birthday, Digital Services Act! – Time for a Reality Check	10/2025	https://algorithmwatch.org/en/birthday-dsa-reality-check/
Papathanasopoulou	From professional fact-checkers to the crowd: can Meta's Community Notes survive the Digital Services Act (DSA)?	10/2025	https://www.tandfonline.com/doi/full/10.1080/13600834.2025.2570974
Amnesty	France: TikTok still steering vulnerable children and young people towards depressive and suicidal content	10/2025	https://www.amnesty.org/en/latest/news/2025/10/tiktok-steering-children-towards-depressive-and-suicidal-content/
Griffin & Fornasari	Risky business? Corporate risk management obligations in sustainability due diligence and digital platform regulation	11/2025	https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risky-business-corporate-risk-management-obligations-in-sustainability-due-diligence-and-digital-platform-regulation/00C87A48A45BE963BDB7852B42A38FB9
Schwertheim, Scheuble & von Bredow (Institute for Strategic Dialogue)	Assessing and Mitigating Conflict-Related Online Risks: Challenges for Governments, Regulators and Online Platforms	11/2025	https://www.isdglobal.org/isd-publications/assessing-and-mitigating-conflict-related-online-risks-challenges-for-governments-regulators-and-online-platforms/

AI Forensics	Prompt, Upload, Repeat: Agentic AI Accounts Flood TikTok	12/2025	https://aiforensics.org/work/agentic-ai-accounts
Albert	What are DSA audits doing for systemic risk enforcement? The case of X	12/2025	https://dsa-observatory.eu/2025/12/19/dsa-audits-what-are-they-good-for/
Bernard	Platforms Report to EU Regulators Under DSA With an Eye on US Politics	12/2025	https://www.techpolicy.press/platforms-report-to-eu-regulators-under-dsa-with-an-eye-on-us-politics/
Rau et al.	Platform badges for civic communication: An interdisciplinary discussion of a risk mitigation measure pursuant to Art. 35 DSA	12/2025	https://policyreview.info/articles/analysis/platform-badges-risk-mitigation
Scott	Assessing What an EU Report Says About Systemic Risks Under the Digital Services Act	12/2025	https://www.techpolicy.press/assessing-what-an-eu-report-says-about-systemic-risks-under-the-digital-services-act/
Seck & Klotsonis (CDT)	How Pornographic Platforms Address Gender-Based Violence Under the DSA	12/2025	https://www.techpolicy.press/how-pornographic-platforms-address-genderbased-violence/
KPMG	Analysis of the 2024/2025 Digital Services Act audit reports	01/2026	https://kpmg.com/nl/en/home/insights/2025/03/kpmgs-2024-digital-services-act-dsa-audit-reports-benchmark.html?1234
Davy	The Missing Metrics in DSA Content Moderation Transparency	01/2026	https://dsa-observatory.eu/2026/01/08/the-metrics-were-missing-in-dsa-content-moderation-transparency/
Oliveira (Unio EU Law Journal)	Algorithmic moderation, shadow banning and systemic risks for media in the European Union: reflections from the first report under Article 35(2) of the Digital Services Act	01/2026	https://officialblogofunio.com/2026/01/26/algorithmic-moderation-shadow-banning-and-systemic-risks-for-media-in-the-european-union-reflections-from-the-first-report-under-article-352-of-the-digital-services-act/
Palumbo	Charting systemic risk management as a regulatory paradigm in EU digital legislation: features, challenges and directions for future research	01/2026	http://lirias.kuleuven.be/retrieve/5b0c53d1-c1bf-4c66-8aa5-3b0fce47452e
Solarova et al. (Kempelen Institute of Intelligent Technologies)	Beyond the Checkbox: Strengthening DSA Compliance Through Social Media Algorithmic Auditing	01/2026	https://arxiv.org/html/2601.18405v1
Gjorgjiev, van Rietschoten & de Vries (KPMG)	Navigating the next phase of the Digital Services Act: audits, Codes of	02/2026	https://www.compact.nl/articles/navigating-the-next-phase-of-the-digital-services-act-audits-codes-

	Conduct, guidelines, and enforcement actions		of-conduct-guidelines-and-enforcement-actions/
Quaritsch (Jacques Delors Centre)	How Has the DSA Performed in Protecting Election Integrity?	02/2026	https://www.techpolicy.press/how-has-the-dsa-performed-in-protecting-election-integrity/
Panoptykon	Brief for the Hearing at the European Parliament on DSA Enforcement and the Protection of Minors	02/2026	https://panoptykon.org/sites/default/files/2026-02/brief-for-the-hearing-at-the-ep-on-dsa-enforcement-and-the-protection-of-minors.pdf
Panoptykon	DSA vs. Reality: Are children safer online?	02/2026	https://en.panoptykon.org/dsa-vs-reality-are-children-safer-online-ep-hearing
Chapman & Steinberg (KGI)	What US Lawsuits Reveal About Platform Design That DSA Reports Don't	02/2026	https://www.techpolicy.press/what-us-lawsuits-reveal-about-platform-design-that-dsa-reports-dont/
Chapman & Steinberg (KGI)	Measuring Risk: What EU Risk Assessments and US Litigation Reveal About Meta and TikTok	02/2026	https://kgi.georgetown.edu/research-and-commentary/measuring-risk-what-eu-risk-assessments-and-us-litigation-reveal-about-meta-and-tiktok/
Isola (DSA Observatory)	How Have Platforms Addressed Addictive Design Under the DSA	02/2026	https://www.techpolicy.press/how-have-platforms-addressed-addictive-design-under-the-dsa/
Jahangir	The Digital Services Act is a Lightning Rod for Debate	02/2026	https://www.techpolicy.press/the-digital-services-act-is-a-lightning-rod-for-debate/
Civil Liberties & EPD	From first to second iteration: civic discourse and electoral processions in DSA risk assessment and mitigation reports	03/2026	https://www.liberties.eu/en/stories/dsa-risk-assessment-epd/45605
Fundación Maldita.es	YouTube Lies: How the Platform Finances Climate Misinformation, Against its Own Policies and the DSA	03/2026	https://maldita.es/investigaciones/20260310/youtube-lies-finances-climate-misinformation-dsa/
WhatToFix	De-Risking Social Media Monetisation. Rating Platforms' Coverage of Monetisation-Related Risks (YEAR 3 DSA Risk Assessment Reports)	03/2026	https://www.whattofix.tech/publications/risk-assessment-reports-monetisation-ratings-2025/
ECNL	Five Critical Lessons from Three Years of DSA Risk Assessments	03/2026	https://ecnl.org/publications/five-critical-lessons-three-years-dsa-risk-assessments
Palmieri, Kollnig & Tamò-Larrieux	Systemic risks of dominant online platforms: A scoping review	04/2026	https://www.sciencedirect.com/science/article/pii/S2212473X26000039

Moore	A New Policy Framework for Governing Collective Sentiment in Online Communities	04/2026	https://www.techpolicy.press/a-new-policy-framework-for-governing-collective-sentiment-in-online-communities/
Baumann, Mein, Pause	Children and Adolescents in the Age of Generative AI – A Framework for Ethical and Educational Governance in Luxembourg	04/2026	https://www.melusinapress.lu/projects/1984-4142