European Union public consultation

Digital Services Act: Summary report of the targeted public consultation on protection of minors guidelines

This document was created from Skimle.com AI-platform from PDF attachments to EU directed public consultation on Protection of Minors Guidelines in relationship to the Digital Services Act.

Public consultation statements (raw data for analysis):
https://ec.europa.eu/eusurvey/publication/DSA_PoM_guidelines

Official EU report: https://ec.europa.eu/newsroom/dae/redirection/document/118211

Our platform provides diverse custom reports and an interactive graphic user interface to consultation data, organized by themes and metadata. We also work together with customers to develop suitable reports in Word, Excel, and PowerPoint formats.

For enquiries on Skimle AI platform, please email info@skimle.com or call Henri Schildt at +358 50 337 12236.

1 Recommendations 6
1.1 Privacy, Data Protection, and Security 6
1.1.1 Privacy by Design and Default 6
1.1.2 Platform Governance and Accountability 10
1.1.3 Legal Compliance and Regulatory Oversight 11
1.1.4 Transparency and User Awareness 13
1.1.5 User Rights and Consent 15
1.1.6 Data Minimisation and Purpose Limitation 16
1.1.7 Data Collection and Sharing 18
1.1.8 Third-Party Access and Commercial Use 19
1.1.9 Sensitive and Special Category Data Safeguards 21
1.1.10 Children's Privacy and Parental Controls 23
1.1.11 Technical Security Measures 26
1.1.12 Blockchain and Decentralised Technologies 28
1.1.13 Miscellaneous 29
1.2 Miscellaneous 30
1.2.1 Business Model Diversity 30
1.2.2 Guideline Examples and Development 30
1.3 Age Assurance and Verification 30
1.3.1 Regulatory Standards and Compliance 31
1.3.2 Risk-Based and Proportionate Approaches 41
1.3.3 Transparency, Oversight, and Governance 49
1.3.4 Privacy, Security, and Data Protection 52
1.3.5 Inclusivity, Accessibility, and Fairness 57
1.3.6 Technical Methods and Innovations 61
1.3.7 Implementation and Ecosystem 66
1.3.8 Miscellaneous 70
1.4 Risk Assessment, Transparency, and Oversight 70
1.4.1 Risk Definitions and Scope 71
1.4.2 Risk Assessment Methodologies and Frameworks 75
1.4.3 Proportionality, Flexibility, and Differentiation 83
1.4.4 Standardization, Certification, and Benchmarks 90
1.4.5 Transparency, Disclosure, and Reporting 93
1.4.6 Oversight, Monitoring, and Accountability 102
1.4.7 Regulatory Integration and Governance 108
1.4.8 Stakeholder Engagement and Collaboration 112
1.4.9 Vulnerable Groups and Special Protections 115
1.4.10 Guidance and Continuous Improvement 118
1.4.11 Miscellaneous 123
1.5 Content Moderation and Harm Prevention 124
1.5.1 Harmful Content Definition and Scope 124
1.5.2 Transparency and Regulatory Compliance 127

1.5.3 Content Moderation Processes and Enforcement 130
1.5.4 User Reporting, Appeals, and Support 134
1.5.5 Algorithmic and Technical Safeguards 139
1.5.6 Contextual and Cultural Adaptation 142
1.5.7 Protection of Minors and Vulnerable Users 144
1.5.8 Addictive and Manipulative Design Features 150
1.5.9 Miscellaneous 153
1.6 Platform and System Design for Child Safety 153
1.6.1 Platform and Ecosystem Responsibility 153
1.6.2 Governance, Accountability, and Regulatory Alignment 157
1.6.3 Transparency and Oversight 160
1.6.4 Safety, Privacy, and Wellbeing by Default 161
1.6.5 Child-Centered and Age-Appropriate Design 167
1.6.6 Mitigation of Manipulative and Addictive Features 172
1.6.7 Content Moderation and Access Controls 177
1.6.8 User Empowerment and Support 181
1.6.9 Miscellaneous 183
1.7 Parental and Guardian Controls 184
1.7.1 Control Settings and Defaults 184
1.7.2 Legal and Regulatory Compliance 187
1.7.3 Consent and Rights Management 189
1.7.4 Parental Guidance and Support 191
1.7.5 Transparency and Communication 194
1.7.6 Content, Activity, and Spending Controls 195
1.7.7 Usability and Accessibility 198
1.7.8 Miscellaneous 199
1.8 Recommender Systems and Personalization 199
1.8.1 Algorithmic Design and System Objectives 199
1.8.2 Profiling, Data Use, and Default Settings 202
1.8.3 User Control and Transparency 206
1.8.4 Platform and Context Specificity 209
1.8.5 Content Diversity and Quality 211
1.8.6 Safety and Risk Mitigation 213
1.8.7 Child and Age-Appropriate Personalization 216
1.8.8 Miscellaneous 219
1.9 AI and Automated System Governance 220
1.9.1 AI Regulation and Legal Compliance 221
1.9.2 Ethical Oversight and Risk Management 223
1.9.3 Transparency and Accountability 225
1.9.4 Fairness and Bias Mitigation 226
1.9.5 User Control and Safety 227
1.9.6 Miscellaneous 230

1.10 User Empowerment, Agency, and Accessibility 230
1.10.1 Inclusive and Accessible Design 230
1.10.2 Transparency and Comprehension 233
1.10.3 User Control and Personalization 236
1.10.4 Participation and Autonomy 240
1.10.5 Freedom of Expression and Rights 242
1.10.6 Healthy Digital Engagement 244
1.10.7 Feedback, Reporting, and Support 245
1.10.8 Miscellaneous 249
1.11 Stakeholder Engagement and Child Participation 249
1.11.1 Inclusive Stakeholder Engagement 249
1.11.2 Diverse and Meaningful Child Participation 252
1.11.3 Feedback and Consultation Mechanisms 256
1.11.4 Safeguards and Specialist Expertise 257
1.11.5 Governance and Oversight 258
1.11.6 Miscellaneous 259
1.12 Education, Awareness, and Digital Literacy 259
1.12.1 Formal and School-Based Digital Literacy 259
1.12.2 Family and Community Engagement 261
1.12.3 Awareness Campaigns and Training 262
1.12.4 Media, Information, and Data Ethics 264
1.12.5 Platform Tools and Safety Features 264
1.12.6 Miscellaneous 266
1.13 Enforcement, Accountability, and Legal Compliance 267
1.13.1 Legal Scope and Regulatory Alignment 267
1.13.2 Roles, Responsibilities, and Coordination 274
1.13.3 Guidance, Proportionality, and Support 278
1.13.4 Accountability, Oversight, and Redress 282
1.13.5 Procedural Clarity and Review 284
1.13.6 Enforcement Mechanisms and Sanctions 287
1.13.7 Miscellaneous 291
1.14 Interoperability, Standards, and Ecosystem Responsibilities 291
1.14.1 Ecosystem Collaboration and Responsibility 292
1.14.2 Standards and Technical Interoperability 294
1.14.3 Guidance and Implementation Support 297
1.14.4 Legal and Regulatory Alignment 298
1.14.5 Competition and User Empowerment 300
1.14.6 Miscellaneous 301
1.15 Advertising, Commercial Practices, and Profiling 301
1.15.1 Legal, Regulatory, and Compliance Frameworks 302
1.15.2 Advertising Standards and Content 304
1.15.3 Data Use, Profiling, and Targeting 307

1.15.4 Protection from Harmful and Manipulative Practices 309
1.15.5 Transparency and Disclosure 313
1.15.6 Influencer and Platform Responsibilities 316
1.15.7 Monetization and Commercial Mechanisms 317

1 Recommendations

The overarching insight from recommendations is the growing consensus that digital environments for minors must embed robust safety, privacy, and empowerment measures by default—making these protections systemic, enforceable, and child-centered, rather than relying on user action or reactive solutions. This is achieved by harmonizing technical, legal, and governance approaches: cross-sector collaboration, unified regulatory frameworks, and interoperability are all repeatedly highlighted as necessary to avoid fragmentation and to ensure that "protective obligations are clear and enforceable for all relevant actors" across the ecosystem. Key points include stringent privacy and data protection, proactive risk assessment, and transparent, accountable governance, especially under frameworks like the DSA, GDPR, and sectoral standards. Stakeholder engagement—where children participate not only as vulnerable users but as "key contributors"—informs policy at every stage, preventing tokenism and ensuring solutions reflect the real needs and rights of minors. Safety features (from parental controls to content moderation) are urged to balance protection with autonomy, involvement, and non-discrimination, and to be accessible, empowering, and inclusive for all children. Meanwhile, advertising, recommender systems, and AI applications are called to move away from profiling and manipulative design, instead foregrounding privacy, transparency, and user agency. A dominant trend is the shift toward flexible, risk-based, and proportionate solutions—responsive to evolving technologies, local contexts, and diverse user needs—underpinned by regular oversight, independent audits, and measurable accountability. Synthesis across sub-categories reveals deep alignment around systemic child protection, inclusive empowerment, and harmonized multi-actor responsibility as foundational pillars for a safer, more rights-respecting digital world for minors.

1.1 Privacy, Data Protection, and Security

The central message across all sub-categories is the elevation of privacy, data protection, and security as foundational principles in digital environments—particularly for minors—requiring that safeguards be embedded "by design and default" at both technical and organizational levels. Platforms are urged to ensure strict controls on data collection, processing, and third-party access, with special emphasis on default privacy settings, minimization of data, and robust technical security measures to protect children's personal and sensitive data. Legal compliance under frameworks like the GDPR and DSA must be harmonized with evolving technological contexts such as blockchain, necessitating clear, context-aware, and proportionate guidance from regulators. Transparent governance, user empowerment—including meaningful consent and easily understandable information—remains key, as does fostering a culture where user rights are respected and privacy risks are clearly communicated. Particular caution is advised against intrusive or manipulative data practices, whether in age verification, recommender systems, profiling, or commercial exploitation of minors' data. A common thread is the call for multi-actor accountability and ongoing review—balancing regulatory requirements, technological innovation, and the “best interest of the child.” Overall, the trend is toward dynamic, risk-based strategies that favor privacy-by-default, user autonomy, and strong oversight rather than prescriptive or technology-specific rules.

1.1.1 Privacy by Design and Default

The insights in the category 'Privacy by Design and Default' consistently advocate for online platforms and digital services to embed privacy, safety, and security as foundational elements in their design and operation, particularly for minors. Key points include setting minors' accounts to the highest or a very high level of privacy by default, restricting content visibility, and ensuring that critical privacy settings are not easily adjustable—especially for younger children. Several documents stress the importance of data minimization, proportionality, and not nudging minors towards lowering privacy safeguards. Technical solutions and early-stage interventions are seen as essential, and distinct privacy, safety, and security requirements should be carefully balanced and, where necessary, disaggregated due to potential conflicts. There is also a focus on clear communication, neutral presentation of choices, and the necessity that privacy safeguards not come at the cost of essential functionalities for minors. A number of contributions note that privacy by design must be both a technical and organizational process guided by established principles (as in the Privacy by Design framework), and that these high standards be enforced even when age estimation or verification processes are in play, always seeking to minimize intrusion and unnecessary data collection.

> *Accounts set to highest privacy by default, with private profiles limiting interactions to accepted contacts only and location settings off.* (Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz))

> *Ensure that the ability to change crucial privacy- by-default settings is not enabled for younger children, especially the visibility of account details, contact restrictions and default recommender*

systems. The specific age where this is recommended may depend on the type of service and the risks identified. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

We agree that accounts of minors should, by default, be set to the highest level of privacy, safety and security. (Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology))

inimum privacy, maximizing data collection Maximize privacy, minimize data collection; Privacy by Design (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Ephemeral messaging provides a clear example of why blanket restrictions on specific features, without appropriate risk context, may not only be disproportionate but also counterproductive to both safety and privacy: (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

Privacy per default", wie bereits in Art 25 der Verordnung (EU) 2016/679 (DSGVO) verpflichtend normiert, sollte hierbei als Standard von Anbietern eingehalten werden. (Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Calls for the adoption of privacy by default settings for minors, such as private profiles, restricted content visibility, and disabling location sharing unless explicitly allowed.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Recommends privacy-by-default settings for minors and urges particular safeguards for younger children, particularly regarding who may contact them and view their information.

Ensure that the ability to change crucial privacy- by-default settings is not enabled for younger children, especially the visibility of account details, contact restrictions and default recommender systems. The specific age where this is recommended may depend on the type of service and the risks identified.

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). Emphasizes privacy as a precondition in designing age estimation solutions, noting potential conflicts between AI-driven age prediction and privacy protection.

The NMA is concerned that effective age estimation by online platforms will be difficult without AI-driven prediction of age and processing of personal data, which may conflict with a high level of privacy.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Advocates embedding privacy by design and by default into platforms, referencing maximizing privacy and minimizing data collection.

The Privacy by Design framework follows seven principles, including privacy as default in platform design.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Reaffirms the application of the Privacy by Design framework in digital services, aiming for minimum data collection and maximum user privacy.

Cavoukian, Ann. 2011. Privacy by Design: The 7 Foundational Principles.

Safe by Default (Panoptykon Foundation). Highlights the need for technical privacy solutions in early design phases, particularly when dealing with unbundling and middleware, to anticipate future privacy risks.

To prevent this scenario, in "Getting Privacy Right" Keller proposed technical solutions, which should be discussed and implemented in early stages of such transformation.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Argues that privacy, security, and integrity protections for minors should not depend on registration and must be universally guaranteed.

These fundamental safeguards must be guaranteed to all minors regardless of whether they have completed a registration process.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Warns against overly intrusive authentication and access barriers, like 'cookie walls', which may reduce usability without effective privacy gain.

A "cookie wall" is another form of access barrier. It refers to the annoying cookie- and privacy- related disclosures presented to readers who access an Internet publisher's service.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Emphasizes that minors' best interests should guide platform design, particularly through robust default privacy and safety settings.

when conducting this review, providers of online platforms accessible to minors should always be guided by the best interests of the minor.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Supports default settings of maximum privacy, safety, and security for minors and highlights behavioral inertia—minors rarely change default configurations.

The guidelines rightly note that minors tend not to change default settings, making defaults critical to their protection (behavioural inertia principle).

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Argues defaults must maximize protection for minors but without restricting core service functionality.

Default settings should be configured to ensure the highest level of privacy, safety and security for minors without unnecessarily restricting access to the core functionalities of a service.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Stresses the importance of 'privacy per default' and data minimization from the point of registration onward.

Weiters sollte der Grundsatz der Datenminimierung im Rahmen des Registrierungsprozesses berücksichtigt werden.

Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology). Supports the automatic application of highest privacy, safety, and security by default for minors but requests clearer policies on adjusting these defaults.

We agree that accounts of minors should, by default, be set to the highest level of privacy, safety and security.

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 (European Commission).

Directs that minors should not be encouraged to weaken privacy settings and encourages providers to apply robust safeguards universally.

Ensure that minors are not in any way encouraged or enticed to change their settings to lower levels of privacy, safety and security.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Promotes secure and neutral default account settings for minors and recommends clarity and prominence in privacy-related controls.

Closely related are account settings, which must privilege secure defaults and avoid subtle pressures that direct minors toward lower privacy options.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Describes company policies to use privacy and safety by design for minors, including high default protections in gaming environments.

The guidelines encourage the use of default settings "to ensure a high level of privacy, safety, and security of minors" (lines 390-391).

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Warns against blanket feature restrictions (e.g., ephemeral messaging), supporting nuanced, privacy-enhancing, and harm-reduction approaches by design.

As with other functionalities referenced in the Guidelines, the impact of ephemeral messaging depends not on its existence, but on how it is implemented. When deployed responsibly, this feature can serve as a privacy-enhancing design choice that reduces the likelihood of long-term harm, including reputational damage, online bullying, and the unauthorized distribution of sensitive content.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Suggests privacy-by-design should aim for high, not necessarily the highest, default settings, with proportional measures aligned with DSA wording.

Consistent with this principle of proportionality, we suggest that the general principle of privacy-, safety- and security-by design should require providers to integrate high (rather than the highest) standards of privacy, safety and security in the design, development and operation of their services.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Highlights the role of established engineering standards for integrating privacy considerations throughout system development.

IEEE 7002TM-2022 Standard for Data Privacy Process contains requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Supports mandatory privacy-by-default for minors and highlights the importance of not nudging them towards weaker protections.

We consider crucial to ensure that children are not nudged towards lowering their settings.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Stresses that age verification must balance correctness with strong data minimization and privacy safeguards.

Data security and data minimization must be top priorities.

Consultation on the Guidelines on Protection of Minors Online under the Digital Services Act (Association for Computing Machinery (ACM)). Recommends separating privacy, safety, and security requirements, noting that enabling privacy and security by design may sometimes conflict.

We feel that privacy, safety and security of minors, which is repeatedly referred to, should be disaggregated.

Consultation Response from Barnevakten, Norway - Regarding Article 28 of the EU Commission's Digital Services Act (DSA) (Barnevakten Foundation). Expresses support for setting the highest privacy settings by default for accounts belonging to children.

Barnevakten supports the requirement that privacy settings must be set to the highest level by default when a child's account is created

1.1.2 Platform Governance and Accountability

This category collates insights that focus on the governance structures and accountability mechanisms that platforms must adopt to ensure a high level of privacy, data protection, and security for minors online—especially as mandated by recent EU legislation. The core expectation is that platforms will establish comprehensive internal governance, including designated responsible staff or teams, effective monitoring and evaluation procedures, and robust, transparent policies to manage minors' data and safeguarding objectives. There is an emphasis on fostering a platform culture of privacy and child participation, informed by well-documented principles and ongoing stakeholder engagement. Platforms are expected to balance the need for data collection (e.g., for age verification or better user experiences) with strong privacy protections, particularly for minors. A principle-based, future-proof approach is advised, complemented by clear processes to govern data ownership, access (especially in cases involving law enforcement), and user control. Coordinated strategies involving state, industry, and civil society, as well as regular reporting and assessment, underpin the drive for robust platform accountability. Representative guidance across the documents stresses that these high-level standards are not just regulatory requirements but fundamental to building a trusted online environment for children, demanding transparency, proportionality, and clarity in both platform policy and practice.

The Commission considers that providers of online platforms accessible to minors should put in place effective governance practices as a means of ensuring a high level of privacy, safety and security for minors on their services for the purposes Article 28(1) of Regulation (EU) 2022/2065. (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 (European Commission))

Companies need comprehensive governance practices to balance the tension between collecting expansive data for business goals and the privacy of users, and especially child users. (II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute))

Adherence to these principles and implementation of corresponding measures are foundational to ensuring a high level of privacy, safety and security for children on online platforms accessible to them. (Public consultation on 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 (Coimisiún na Meán))

Ensure that while blocked content is no longer accessible to the child, a secure log is retained for legal authorities upon justified request (e.g. police reports or child protection services). (Feedback DSA (unknown))

There is tension between collecting data for safer experiences and preserving privacy of minors. (II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute))

Service providers are obliged to ensure that the protection objective is warranted and provide on option to report violations of personal integrity. (On the concept of personal integrity in the german protection of minors (unknown))

Public consultation on 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 (Coimisiún na Meán). Emphasizes the necessity for platforms to assign responsibility for child privacy and safety to specific teams, foster a culture of child participation, and adopt transparent monitoring and evaluation methods to ensure ongoing effectiveness of protective measures.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Stresses the tension between expansive data collection for business needs or safety tools and the fundamental privacy rights of minors, urging comprehensive governance to manage these conflicts.

Companies need comprehensive governance practices to balance the tension between collecting expansive data for business goals and the privacy of users, and especially child users.

Feedback DSA (unknown). Focuses on governance issues around the retention and ownership of sensitive data (like interaction histories) when it is required for legal or protective reasons, and calls for clearer provisions on age-related data accountability.

This raises serious concerns about data governance: who ultimately controls this sensitive, private information? It cannot and should not be solely Google.

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 (European Commission). Outlines the need for platforms accessible to minors to foster a culture of privacy and child participation, and to formally integrate privacy and safety objectives into governance through systematic monitoring and internally enforced policies.

The Commission considers that providers of online platforms accessible to minors should put in place effective governance practices as a means of ensuring a high level of privacy, safety and security for minors on their services for the purposes Article 28(1) of Regulation (EU) 2022/2065.

On the concept of personal integrity in the german protection of minors (unknown). Highlights German regulatory requirements for service providers to facilitate reporting of violations and for collaborative, regular assessment among government, industry, and civil society of personal integrity protections for minors.

17a states that the realisation of the protection objectives should be promoted through a joint assumption of responsibility by the state, industry and civil society to coordinate an overall strategy.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Expresses strong NGO support for DSA guidelines ensuring robust platform-level privacy, safety, and security for minors, viewing these as crucial for trustworthy online environments.

Together with the 27 undersigning organisations and experts from across Europe, we strongly support the draft guidelines on Article 28(1) of the Digital Services Act (DSA), which require platforms accessible to minors to ensure a high level of privacy, safety and security.

INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego). Presents the EU Commission’s guidelines as an important reference for platforms, specifying that adequate and proportionate measures be enacted to uphold minors' privacy and safety, with the guidelines forming the benchmark for regulatory compliance.

Las directrices de la Comisión Europea tienen por objeto describir " ... las medidas que la Comisión considera que los proveedores de plataformas en línea accesibles a menores deben adoptar para garantizar un alto nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 1, del Reglamento (UE) 56 2022/2065 del Consejo y del Parlamento."

1.1.3 Legal Compliance and Regulatory Oversight

The documents in this category focus on the legal compliance and regulatory oversight aspects of privacy, data protection, and security—particularly as they pertain to minors online and the obligations of digital service providers within the EU regulatory framework. The key insights revolve around the application and interpretation of the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), ensuring that online platforms implement proportionate, effective, and state-of-the-art measures to safeguard minors' privacy and security. Notably, these guidelines require platforms, especially very large online platforms (VLOPs) and search engines (VLOSEs), to perform comprehensive and nuanced risk assessments when applying protective measures, balancing children's rights, technological effectiveness, and regulatory proportionality. Emphasis is placed on not only compliance with EU-wide legislation, such as the DSA and GDPR, but also the need for interoperability, regular compliance monitoring, and harmonization with national and sector-specific standards. A further area of insight addresses the delineation of responsibilities in legal

compliance, advocating for competent authorities, rather than individual online platforms, to make determinations regarding the intrusiveness and legal adequacy of privacy-protective tools. This recognizes limitations in platform expertise and mitigates undue regulatory burden, especially for technical actors like blockchain node operators who typically lack discretion over data processing. The insights also underscore the value of context-sensitive, risk-based approaches, including Data Protection Impact Assessments (DPIAs), and the necessity for audience measurement and age verification tools to comply with established privacy and data protection obligations. Collectively, the documents advocate for a cooperative, multi-actor approach to regulatory compliance, robust oversight mechanisms, and the evolution of best practices to adapt to emerging challenges in protecting minors' online privacy and data rights.

> *As indicated in the Introduction of these guidelines (section 1, page 4), certain provisions of Regulation (EU) 2022/2065 including Section 5 of Chapter III impose additional obligations on providers of very large online platforms ("VLOPs") and very large search engines ("VLOSEs").* (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 (European Commission))
>
> *Proportionality: Article 28(1) of Regulation (EU) 2022/2065 requires any measure taken to comply with that provision to be appropriate and proportionate to ensure a high level of privacy, safety, and security of minors.* (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 (European Commission))
>
> *Ensuring the processing of personal data is lawful, fair, and transparent.* (How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition))
>
> *Classifying nodes as controllers risks deterring participation in decentralised systems and could inadvertently undermine the privacy benefits that decentralisation itself provides.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))
>
> *Apply regardless of the device or operating system used to access the service.* (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 (European Commission))
>
> *Ensuring that any technological and organisational solutions employed to implement these guidelines are 'state-of-the-art' and are aligned with national guidance on the protection of minors (63) and the highest available standa* (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 (European Commission))

Public consultation on 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 (Coimisiún na Meán). This document recommends clarifying that the privacy and safety guidelines for minors reflect not just the European Commission's views but are also shaped by Digital Services Coordinators (DSCs) and the regulatory cooperative process.

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). It advocates for GDPR carve-outs and nuanced classification for blockchain technical actors like node operators, arguing that passive infrastructure players should not automatically be considered data controllers due to their limited influence over personal data processing.

Therefore, the Guidelines should make clear that operating a node, in itself, does not equate to controllership.

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 (European Commission). The Commission establishes that VLOPs and VLOSEs must implement proportionate, risk-based protective measures for minors, accounting for the full spectrum of their DSA obligations while integrating national guidance and evolving technological best practices.

Proportionality: Article 28(1) of Regulation (EU) 2022/2065 requires any measure taken to comply with that provision to be appropriate and proportionate to ensure a high level of privacy, safety, and security of minors.

Feedback for 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 (xHamster). This feedback emphasizes that the responsibility for assessing the intrusiveness and legality of privacy protections—especially those that are technically complex or potentially intrusive—should rest with competent authorities, not individual platforms.

Providers of online platforms may lack the legal and technical expertise required to make such assessments, especially considering that the proposed methods are highly intrusive ab initi

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). The institute underscores the importance of following the Commission's guidelines under the DSA to ensure minors' online privacy, safety, and security, reinforcing legal compliance as critical for all actors.

Commission. "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."

On the concept of personal integrity in the german protection of minors (unknown). It highlights the interplay between German law, EU data protection, and audiovisual directives in offering broad protection to minors' personal integrity online, recognizing the comprehensive scope of EU fundamental rights.

The EU Audiovisual Media Services Directive 14 also protects minors from the disclosure of their personal data for commercial purposes15 and stipulates that audiovisual commercial communications must not lead to physical, mental or moral harm to mino

How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition). This document stresses adherence to overarching data protection, privacy, and security obligations—like DPIAs and EDPB guidance—when deploying audience measurement for age verification of minors online.

Ensuring the processing of personal data is lawful, fair, and transparent.

1.1.4 Transparency and User Awareness

This collection of insights emphasizes the importance of transparency and user awareness, particularly for minors, in online environments. Key measures include providing clear and accessible information about privacy risks, especially when engaging with AI features or altering privacy settings. Communication must be age-appropriate, ensuring minors understand how their data and interactions may be used, shared, or disclosed to others. Visual privacy indicators, such as a traffic light system, are recommended to help children perceive privacy impacts in real time. Additionally, platforms are encouraged or required to accurately inform both minors and guardians about the implications of privacy-related actions, such as the increased risks from making accounts public. The feedback also stresses the need for responsible privacy policies that go beyond mere compliance, including clear safety warnings, transparent handling of reports or complaints, and effective user redress mechanisms. There is acknowledgement that onerous requirements for disclosure of personal information can deter users, especially due to fears of identity theft or fraud, thus potentially undermining the overall openness of online spaces.

Communicate in an age-appropriate and transparent manner how any interaction or information shared by the user is used by the service. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Visual cues (e.g. a traffic light system) can help minors understand how their privacy level changes when adjusting settings. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

There should be a requirement to accurately disclose to minors, and guardians where applicable, the risk implications of changing the default privacy settings, in particular if that introduces new risks to the account. (European Commission Article 28 Guidelines Feedback (unknown))

Requiring Internet users to provide . . . personally identifiable information to access a Web site would significantly deter many users from entering the site, because Internet users are concerned about security on the Internet and . . . afraid of fraud and identity theft[.]" (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

There should be a requirement to accurately disclose to minors, and guardians where applicable, the risk implications of changing the default privacy settings, in particular if that introduces new risks to the account. (European Commission Article 28 Guidelines Feedback (unknown))

Signatories agree to support awareness of parental controls and to take account of children's' perspectives, needs, interests and rights during product/service design. (Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Advocates for platforms to clearly label AI features, explaining privacy risks and the fate of shared information for user awareness.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Emphasizes age-appropriate, transparent communication to minors about how their data and activities are used by services.

Communicate in an age-appropriate and transparent manner how any interaction or information shared by the user is used by the service.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Highlights that requiring personal information for website access can significantly deter users due to security concerns and fear of identity theft.

Requiring Internet users to provide . . . personally identifiable information to access a Web site would significantly deter many users from entering the site, because Internet users are concerned about security on the Internet and . . . afraid of fraud and identity theft[.]"

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Recommends visual cues, such as a traffic light system, to help minors understand privacy implications of settings adjustments.

Visual cues (e.g. a traffic light system) can help minors understand how their privacy level changes when adjusting settings.

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 (European Commission). Calls for easy access and clear explanations to minors about what information related to their reports or complaints is shared and with whom.

Where providers of online platforms share information with others, they should explain to minors when, how and what information related to reports and/or complaints they share with other users or third parties.

European Commission Article 28 Guidelines Feedback (unknown). Proposes mandatory and accurate disclosure of additional risks to minors and guardians when changing privacy defaults, especially if public exposure introduces new threats.

There should be a requirement to accurately disclose to minors, and guardians where applicable, the risk implications of changing the default privacy settings, in particular if that introduces new risks to the account.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). Focuses on the importance of maintaining responsible privacy policies, safety warnings, and redress mechanisms, while also supporting parental controls and children's rights.

The Code also includes specific commitments relating to privacy policies, illegal and harmful content, safety warnings, community standards and complaints, consumer redress mechanisms and monetisation.

1.1.5 User Rights and Consent

The insights within the 'User Rights and Consent' category highlight critical issues around safeguarding individuals' control over their personal data. Key themes include the challenges of upholding the right to erasure and rectification in immutable environments like blockchain, where technical limitations may require alternative solutions such as data obfuscation or key deletion, balanced with compliance and transparency needs. The importance of ensuring that platforms, especially those using recommender systems and targeting, prioritize privacy and informational self-determination is underscored by concerns about data exploitation in profiling and surveillance-driven business models. Special attention is given to children and vulnerable populations, emphasizing the prevention of manipulative data prompts during registration and accounting for privacy and security concerns in compliance processes like age verification. Additionally, the adoption of standards for machine-readable privacy terms is proposed to enhance transparency and user agency in consent processes. Collectively, the documents advocate for interpretive and technical guidance that balances user rights with legitimate regulatory and public interests, urges design choices that respect privacy, and emphasizes the need to empower users—particularly minors—to make informed and voluntary decisions regarding their data.

For instance, rendering data inaccessible through methods like key deletion or cryptographic obfuscation could, in certain scenarios, fulfil the intent of Article 17. (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

Last but not least, platforms' choices to optimise for content which is likely to engage users facilitates invasive harvesting and exploitation of users' personal data, in order to profile them for recommendations and sponsored content. (Safe by Default (Panoptykon Foundation))

Children should never be pushed during the registration process to disclose more personal information than necessary or to opt into settings that compromise their privacy. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

The continued storage of data on a blockchain may thus be not only legitimate but also required by law, including in diverse contexts such as legal certainty, traceability, or the prevention of misuse. (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

Amnesty International argues that this is a serious and recurrent interference with people's right to privacy: (Safe by Default (Panoptykon Foundation))

over 99% of users subjected to a verification requirement did not verify their age"). (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). This document discusses the tension between blockchain immutability and users' GDPR rights, recommending alternative solutions for erasure and rectification and a risk-based approach to controller compliance within legal constraints.

For instance, rendering data inaccessible through methods like key deletion or cryptographic obfuscation could, in certain scenarios, fulfil the intent of Article 17.

Safe by Default (Panoptykon Foundation). Highlights concerns about the exploitation of users' personal data in content recommendation and targeting systems, emphasizing the threat to privacy and informational self-determination due to pervasive profiling practices.

Last but not least, platforms' choices to optimise for content which is likely to engage users facilitates invasive harvesting and exploitation of users' personal data, in order to profile them for recommendations and sponsored content.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Stresses the need for child protection online by prohibiting platforms from coercing children into sharing unnecessary personal information or opting for privacy-compromising settings during registration.

Children should never be pushed during the registration process to disclose more personal information than necessary or to opt into settings that compromise their privacy.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Points out that privacy and security apprehensions can significantly deter users from complying with age verification processes, as demonstrated by high drop-off rates.

over 99% of users subjected to a verification requirement did not verify their age").

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Proposes the use of machine-readable personal privacy terms to enable transparent and automatable consent processes for the protection of minors' data.

EEE P7012TM Standard for Machine Readable Personal Privacy Terms identifies/addresses the manner in which personal privacy terms are proffered and how they can be read and agreed to by machines.

1.1.6 Data Minimisation and Purpose Limitation

The insights across these documents strongly emphasize the foundational data protection principles of data minimization and purpose limitation—particularly in the context of protecting minors online. Stakeholders argue that platforms should collect and process only the data strictly necessary to provide services, especially when dealing with children's information, and should proactively prevent the secondary use or further processing of such data. Registration processes should limit required information to essentials (e.g., name, age, guardian's email) and avoid nudging minors to provide excess details. Several submissions warn against 'function creep,' especially with age assurance and verification tools, making clear that collected data should not be repurposed for advertising, behavioral analysis, or identity verification. There is also a call for platforms to implement privacy-by-default configurations and not to collect additional personal data solely to assess a user's age, in alignment with recent EU regulations. Flexibility is acknowledged—settings and data requirements may vary depending on the platform's features and risk profiles—but respondents widely agree that any data collection must remain within strict necessity. Moreover, technical measures supporting these goals, and reference to GDPR and data-protection-by-design principles, are recommended to further reinforce limitations on data usage.

This is why minimisation of the data collected becomes of paramount importance, in that it cuts the data and transmission down to what is absolutely necessary and in doing so it reduces data's exposure to risk. (CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.))

Comply with data protection principles as stated by EDPB in its statement, including data minimisation (General Data Protection Regulation (GDPR) Art. 5(1)(c)) and UNCRC Article 16 (right to privacy). (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

The necessary information should be limited to the user's name, age, and guardian's contact email address, with no optional/additional tabs for personalised experience purposes." (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

This is why minimisation of the data collected becomes of paramount importance, in that it cuts the data and transmission down to what is absolutely necessary and in doing so it reduces data's exposure to risk. (CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.))

These variations are necessary to account for each platform's unique userbase, purpose, features, and risk profile. (Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Argues for strict limits on the further use of geolocation and similar data collected from minors, insisting that platforms must not continue using such sensitive information after a session ends.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Highlights how data minimization is crucial for protecting minors—citing risks of lifetime harm from breaches—and critiques data proliferation. Stresses reduction of collected/transmitted data to essentials only.

This is why minimisation of the data collected becomes of paramount importance, in that it cuts the data and transmission down to what is absolutely necessary and in doing so it reduces data's exposure to risk.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Advocates for prevention of secondary data uses ('function creep') in age assurance, stressing that such data must not serve advertising, identity, or behavioral purposes. Reiterates strict adherence to data minimization and rights-based frameworks.

Comply with data protection principles as stated by EDPB in its statement, including data minimisation (General Data Protection Regulation (GDPR) Art. 5(1)(c)) and UNCRC Article 16 (right to privacy).

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 (European Commission). Clarifies that platforms are not required to collect or process extra personal data beyond what is necessary to assess a user's age, reinforcing data minimization obligations for services accessible to minors.

Paragraph 3 specifies that compliance with the obligations set out in Article 28 shall not oblige providers of online platforms accessible to minors to process additional personal data in order to assess whether the recipient of the service is a minor.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Stresses the importance of avoiding registration processes that nudge minors to share more than necessary; specifies that only the minimal required information (name, age, guardian’s email) should be collected.

The necessary information should be limited to the user's name, age, and guardian’s contact email address, with no optional/additional tabs for personalised experience purposes.”

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). Supports privacy-by-default for minors, but calls for recognition of variation in how platforms implement default settings, emphasizing that only essential data should be collected for service provision.

Additionally, it is important for the Commission to clarify in the Guidelines that, when implementing default settings, services should not be required to collect information beyond what is necessary for the provision of the service.

Consultation on the Guidelines on Protection of Minors Online under the Digital Services Act (Association for Computing Machinery (ACM)). Urges direct application of GDPR principles like data minimization and purpose limitation in the design of age verification processes, suggesting technical exemplars for enforcing these principles.

ne way to achieve such a goal would be to directly invoke principles such as data minimisation or purpose limitation from the GDPR8 in the context of data collected for performing said verification, together with introducing exemplary technical methods that can support the goal.

INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego). Restates that platforms have no obligation to process additional data to determine if a user is a minor, per Article 28, thus supporting core data minimization standards.

El cumplimiento de las obligaciones establecidas en el presente artículo no obligará a los prestadores de plataformas en línea a tratar datos personales adicionales a fin de evaluar si el destinatario del servicio es un menor.

1.1.7 Data Collection and Sharing

This category examines the challenges and proposals related to data collection and sharing within the context of privacy, data protection, and security. Key insights include the need for clearer regulatory guidance when dealing with decentralized environments such as blockchain networks, where traditional notions of data transfers and compliance mechanisms are difficult to apply due to the lack of identifiable data recipients and geographical boundaries. Recommendations include adopting risk-based, proportional approaches to enforcement and considering technical and organizational safeguards. For minors' privacy, submissions emphasize the necessity of refining data collection provisions to prohibit intrusive logging (such as full-funnel attention tracking), while still supporting essential systems through privacy-preserving techniques such as ephemeral or aggregated logs protected with differential privacy. Furthermore, clear guidance is sought to resolve operational tensions between minors' autonomy and parental oversight in data collection, especially concerning non-profiling recommendations and recommender system resets. Lastly, the need for a standardized, robust definition of contextual advertising is advocated, especially for protecting minors online. The lack of clarity around such definitions under EU law has led to inconsistent privacy protections. By referencing best-practice definitions, platforms and regulators can better ensure strong, uniform privacy safeguards against profiling-based advertising.

Current mechanisms for international data transfers were designed with centralised data exchanges in mind. Their application in open networks, where data may be propagated to unknown entities in unknown jurisdictions is highly impractical. (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

Clarify the data collection provisions: Refine the ongoing data-use restrictions to clearly prohibit full-funnel attention logging (e.g. dwell time, infinite scroll traces), while explicitly allowing (i) ephemeral, on-device processing or (ii) aggregated logs subject to differential privacy protections. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

In order to ensure the highest level of privacy protection for minors and to avoid a fragmented interpretation of what non-profiling advertisement can be, we suggest that the guidelines reference the definition of contextual advertising above as a best practice example that companies can follow to be compliant. (CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)))

The Guidelines should acknowledge this gap and provide interim solutions or endorse alternative approaches (e.g., contractual obligations at the application layer, technical access restrictions, or architectural segregation between EEA and non-EEA nodes). (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

The provision enabling users to reset recommender systems and the option for minors to select non profiling based recommendations present operational challenges for compliance with audit trail requirements and parental oversight mechanisms. (HOMO DIGITALIS CONTRIBUTION TO THE

EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

One privacy-respecting alternative to profiling-based advertising that is often proposed is contextual advertising. (CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)))

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). This document addresses the complications of applying international data transfer regulations to blockchain technologies, highlighting the impracticality of current mechanisms and proposing the need for tailored frameworks and clarity around what constitutes a data transfer in decentralized settings.

Current mechanisms for international data transfers were designed with centralised data exchanges in mind. Their application in open networks, where data may be propagated to unknown entities in unknown jurisdictions is highly impractical.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). The submission calls for more precise restrictions on data collection relating to minors, advocating clear prohibition of certain forms of behavioral tracking and recommending privacy-enhancing methods for necessary data processing, while seeking alignment between minor autonomy and parental oversight in data collection practices.

Clarify the data collection provisions: Refine the ongoing data-use restrictions to clearly prohibit full-funnel attention logging (e.g. dwell time, infinite scroll traces), while explicitly allowing (i) ephemeral, on-device processing or (ii) aggregated logs subject to differential privacy protections.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). The response urges referencing a privacy-focused definition of contextual advertising in EU guidelines to address inconsistencies in privacy protections for minors and to support economic sustainability for news media without relying on profiling.

In order to ensure the highest level of privacy protection for minors and to avoid a fragmented interpretation of what non-profiling advertisement can be, we suggest that the guidelines reference the definition of contextual advertising above as a best practice example that companies can follow to be compliant.

1.1.8 Third-Party Access and Commercial Use

This category centers on the imperative to rigorously restrict third-party access and commercial use of minors' data, particularly in digital platforms and services. Core insights include the need to implement default protections that prevent the sharing and processing of children's data by third-party entities, unless strictly necessary and compliant with robust child data protection standards. Platforms are urged to map, assess, and disclose data-sharing practices with third parties to ensure transparency and accountability, in line with GDPR-like frameworks. There is also a strong consensus among stakeholders for prohibiting the use of data collected for age estimation or verification—such as biometrics or behavioral profiles—for any commercial purposes, including profiling, targeted advertising, and direct marketing. Moreover, heightened scrutiny is advised in the context of scraping or other unintended commercial/ciminal access to minors' data. Service providers are recommended to introduce child-centric safeguards: setting user profiles private by default, blocking discoverability, and providing child-friendly support and reporting mechanisms to minimize third-party exploitation risks.

Furthermore, there is no mention of third-party data flows, representing a significant privacy gap. Default settings should govern not only platform features but also control data exposure to third parties, including advertisers and analytic tools, to ensure comprehensive protection of minors' privacy rights. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Ab Zeile 277: Aus Konsumentenperspektive ist sicherzustellen, dass technische oder KI-unterstützte Methoden zur Altersschätzung, die personenbezogene Daten von Minderjährigen, die von den Plattformanbietern erhoben oder anderweitig gewonnen werden, nicht für kommerzielle Zwecke, wie etwa Direktwerbung, Profiling und auf das Nutzungsverhalten abgestimmte Werbung verwendet werden. (Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)))

Die damit erhobenen Daten sollen nicht für kommerzielle Zwecke (z. B. personalisierte Werbung) verwendet werden. (ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)))

Furthermore, there is no mention of third-party data flows, representing a significant privacy gap. Default settings should govern not only platform features but also control data exposure to third parties, including advertisers and analytic tools, to ensure comprehensive protection of minors' privacy rights. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Require platforms to map and assess data-sharing practices with third parties that could impact minors' privacy or security, similar to the GDPR obligations. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

It is also recommended to set user profiles in such a way that they cannot be found by search services and that their location, contact details and communication are blocked. (On the concept of personal integrity in the german protection of minors (unknown))

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis recommends extending privacy and security protections to cover third-party integrations and ensuring platforms conduct thorough data governance and risk assessments relating to third-party data flows impacting minors.

Furthermore, there is no mention of third-party data flows, representing a significant privacy gap. Default settings should govern not only platform features but also control data exposure to third parties, including advertisers and analytic tools, to ensure comprehensive protection of minors' privacy rights.

Feedback DSA (unknown). This feedback emphasizes strict limitations on third-party scraping of minors' content, noting heightened risks when content is harvested for commercial or criminal intent.

Restrict scraping of minors' content by third parties—particularly for commercial use or for criminal purposes like pedocriminality.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). BMASGPK stresses that data collected for age estimation via technical or AI-supported means should not be repurposed for commercial uses such as advertising or profiling, highlighting particular dangers associated with increased reliance on AI.

Ab Zeile 277: Aus Konsumentenperspektive ist sicherzustellen, dass technische oder KI-unterstützte Methoden zur Altersschätzung, die personenbezogene Daten von Minderjährigen, die von den Plattformanbietern erhoben oder anderweitig gewonnen werden, nicht für kommerzielle Zwecke, wie etwa Direktwerbung, Profiling und auf das Nutzungsverhalten abgestimmte Werbung verwendet werden.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). ÖIAT underlines that data acquired for age

verification must be strictly limited to that use alone and never exploited for commercial activities such as personalized advertising.

Die damit erhobenen Daten sollen nicht für kommerzielle Zwecke (z. B. personalisierte Werbung) verwendet werden.

On the concept of personal integrity in the german protection of minors (unknown). This document calls on service providers monetizing minors' data to adopt proactive child-safety measures, including privacy-centric default settings, content and contact controls, and the prohibition of unauthorized data transfers.

The restriction of contact to a group of people selected by the users themselves, as well as anonymous or pseudonymous usage of services, the prohibition of the transfer of usage data and the provision of child-friendly general terms and conditions shall protect young people when using digital services.

1.1.9 Sensitive and Special Category Data Safeguards

The insights in the category 'Sensitive and Special Category Data Safeguards' highlight the imperative to rigorously protect minors' personal and sensitive data, especially in the context of digital platforms, AI systems, and regulatory compliance. There is strong consensus on prohibiting or severely restricting the use of children's data—including chatbot interactions, photos, and videos—for AI training or profiling purposes, and ensuring that any such processing always requires explicit or informed consent. Various submissions emphasize the heightened sensitivity of biometric, geolocation, and behavioral data, citing the need for stringent privacy measures and default protections that align with GDPR, particularly Article 9 regarding special category data. Privacy and anonymity in age assurance solutions, including both verification and estimation, are recurrent themes. Recommendations include double anonymity practices—ensuring neither platforms nor verifiers can link a child's identity to online actions—and the importance of third-party, independent operation of verification mechanisms. There are also cautions against regulatory pressures incentivizing more invasive or excessive data collection from minors, highlighting that such practices could be counter-productive for child safety. Furthermore, the protection of minors' ability to seek help confidentially, safeguards against misuse or economic exploitation of data, and calls for a broad interpretation of personal integrity (incorporating informational self-determination) are stressed as central to a rights-based, comprehensive approach to children's data protection.

Interactions between children and chatbots should also not be used to track children's data or feed such data into the training of AI systems. (SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International))

Specify that alternative age verification methods to the EUDI Wallet, in addition to ensuring an equivalent level of verification, must ensure equivalent levels of privacy corresponding to the principle of "double anonymity." (AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)))

En effet, les données à caractère personnel relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique sont particulièrement protégées par l'article 9 du règlement général sur la protection des données (RGPD) ; (Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom))

It would be appropriate, in AGCOM's opinion, to add that age estimation techniques, unlike age verification, can also be based on the acquisition of information sensitive to user privacy, such as behavioral data or biometric data, which are processed by automated systems to establish, with a certain margin of accuracy, the age or age range of the user. (AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)))

Children may fear being monitored or punished for reporting. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

The abuse of inexperience and age, economic exploitation and the commercial or other improper processing and dissemination of user data are, conversely, contrary to the protection of personal integrity. (On the concept of personal integrity in the german protection of minors (unknown))

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Highlights the need to prevent the use of data arising from children's chatbot interactions for tracking or as training data in AI systems, promoting higher privacy standards for minors.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Stresses the privacy challenges in age estimation and verification, advocating for methods that uphold 'double anonymity' so neither platform nor verifier knows the full identity or platform usage of the user.

Specify that alternative age verification methods to the EUDI Wallet, in addition to ensuring an equivalent level of verification, must ensure equivalent levels of privacy corresponding to the principle of "double anonymity."

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Warns against regulatory approaches that inadvertently encourage the collection of more sensitive minors' data by online publishers, underscoring minimal collection as a protective strategy.

Reminder: it does not benefit minors to motivate publishers to collect more sensitive information from minors.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Calls for the restriction of minors' geolocation tracking and sharing by default, alongside clear notifications about any such data handling.

restrict the sharing of the geolocation of the minor and provide notice regarding the tracking of the minor's geolocation.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Emphasizes the importance of confidentiality in help-seeking scenarios for minors, ensuring that privacy is maintained and that disclosures do not trigger abuser alerts.

Their ability to seek help must be protected by confidentiality assurances, including not alerting abusers (in domestic violence or coercion situations).

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Argues that children's data should not be used in training AI models, insisting on explicit user consent for any data-driven AI development.

Providers of online platforms should not use data of children to train their Al models.

Feedback DSA (unknown). Advocates for sensitive data of minors to be hidden by default, even from 'approved' contacts, and prohibits using minors' data for AI training without explicit permission.

Sensitive data (e.g., phone number, geolocation) should be hidden by default, even from "approved" contacts, unless explicitly permitted, rather than automatically to all approved contacts.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Reinforces the necessity for independent and privacy-focused age verification systems under DSA, especially for services like pornography, and recognizes the special protection requirements for sexual data under GDPR.

En effet, les données à caractère personnel relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique sont particulièrement protégées par l'article 9 du règlement général sur la protection des données (RGPD) ;

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Recommends outright prohibition on using children's data for AI training as a protective regulatory measure.

Möglich Maßnahme: Die Nutzung von Daten von Kindern für das KI-Training soll verboten sein.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). States that age assurance solutions must strictly adhere to privacy standards stipulated in Article 9 GDPR concerning special category data.

Ensure the privacy of age assurance solutions in line with article 9 of the GDPR.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Discusses the challenges of lawfully processing special category data when consulting minors and calls for engagement with DPAs for clear compliance guidance.

To support safe and lawful implementation, we would therefore suggest that the Commission considers engaging with DPAs to provide clearer guidance on how such processing can be conducted in compliance with data protection obligations.

On the concept of personal integrity in the german protection of minors (unknown). Advocates for a broadening of the concept of minors' personal integrity to explicitly include digital and data protection alongside physical and mental protection.

However, new voices are calling for regulations that do not differentiate between the integrity of the human individual and the inseparably associated data.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Clarifies that age estimation using biometric data is highly invasive, and such processing involves special categories of personal data requiring heightened protection under GDPR.

Wir möchten darauf hinweisen, dass es sich bei diesen Daten um besondere Kategorien personenbezogener Daten im Sinne von Art. 9 der Datenschutz-Grundverordnung handelt.

1.1.10 Children's Privacy and Parental Controls

The insights across these documents reflect a comprehensive approach to children's privacy and parental controls in digital environments. A central theme is the prioritization of a high level of privacy, safety, and security for minors by design, including strict defaults for privacy and limitations on data collection practices. Guidelines emphasize that children's rights to privacy must not depend solely on parental controls, and that privacy tools and settings should evolve with age and maturity, offering age-appropriate autonomy and protection. Key recommendations include restricting the collection and use of sensitive data such as precise geolocation, prohibiting unsafe AI-generated prompts, ensuring strict controls over the sharing of minors' data (including in social media and influencer contexts), and resisting intrusive verification measures such as mandatory government ID submission. The need for clearly distinguishing between privacy settings that must remain fixed versus those that may adapt as children grow is highlighted, as is the importance of clear lines of responsibility and transparent enforcement. There is a call for privacy and safety measures to be balanced against the child's autonomy and rights, underpinned by GDPR principles like data minimization and considering the best interest of the child. Representative feedback further stresses practical measures, such as tools for reporting or removing unwanted content, and calls for robust enforcement of privacy and data protection rules tailored to the realities of children in digital spaces.

Bris therefore emphasizes that a child's right to a high level of privacy, security, and safety must never depend on guardian control. (Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris))

The guidelines should draw a clear line between settings that must remain disabled and unchangeable for minors (such as location sharing, unsolicited contact, activation of microphones or cameras without a clear and temporary session-based prompt, or the public display of follower or friend lists) and those settings which can be adapted over time as children grow older and their needs change, provided such changes are guided neutrally and safely. (Missing Children Europe Submission Public

Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

the default setting must commence with the most restrictive configuration for privacy, safety, and security, until further assurance permits relaxing the safeguards. (IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)))

We also welcome the clear integration of children's rights principles throughout the text, and the strong focus on implementation and enforcement that reflects the DSA's vision of a safe, trusted digital environment. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

b) Default settings: clarify which of the settings children should have control over depending on their evolving capacity and ensure that children are not nudged towards lowering their settings. (STATEMENT (Digipeace (Digirauha ry)))

The language of the guidelines needs to be reinforced in this sense. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Advocates for ensuring AI-generated responses do not prompt minors to share personal information, reinforcing safeguards in AI-assisted interactions with children.

Contribution Guidelines art 28 DSA (Respect Zone). Stresses the need for platforms targeting minors to prevent the sharing of personal data and restrict interactions to within intended communities.

They must prevent minors from sharing personal data or interacting with users outside the intended community;

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Encourages adherence to data minimization under GDPR and highlights the risk from business models reliant on data collection from children.

Adhere to the data minimisation principles included in the GDPR, avoiding practices that attempt to extract more data that that in the best interests of the child

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Calls for explicit inclusion in DSA guidelines of risks related to children's data use, especially with chatbots, warning against gaps if AI regulation is rolled back.

Including language in the DSA Guidelines to this effect is crucial amidst the current discussions of a pause or even rollback of AI regulation in the European Union, which risks leaving critical risks to children's rights unaddressed.

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Explores children's experiences with online privacy and the effectiveness of privacy strategies, including dealing with unauthorized image sharing.

Strategies: Making profiles private, avoiding sharing content, and using platform functions to remove or report unwanted content.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Urges a distinction between precise and general geolocation, justifying the need for certain geolocation data to support legal compliance and online safety for minors.

However, it is important to distinguish between precise and general (or non-specific) geolocation.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Supports enabling only non-precise geolocation by default, tying general location data to legal obligations and fraud prevention while restricting tracking of minors.

It is important, however, to differentiate between exact and general or non-precise geolocation features.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Emphasizes that the right of children to privacy and safety online should be unconditional and not depend on the actions of guardians or parents.

Bris therefore emphasizes that a child's right to a high level of privacy, security, and safety must never depend on guardian control.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Calls for clarity on behavioral data collection from minors on platforms and recommends age-differentiated approaches to enhance self-determination for older minors.

If the platform can, in principle, also be used by minors, it is necessary to clarify under what conditions behavioural data may be collected.

Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children). Requests clarification on which parties are responsible for ensuring minors are not encouraged to lower privacy settings and suggests more explicit guideline language.

The proposed guidelines indicate that providers should "Ensure that minors are not in any way encouraged or enticed to change their settings to lower levels of privacy, safety and security" (line 430). This guideline needs clarification.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Advocates for treating privacy and security as jointly essential in processing children's data and tailoring protective mechanisms in the online environment.

While ensuring a high level of confidentiality, it is essential to give online platforms the opportunity to implement the best mechanisms for the security and protection of minors on the Internet.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Proposes clear rules for unchangeable privacy settings for sensitive features and supports strong privacy and safety mandates for platforms accessible to minors.

The guidelines should draw a clear line between settings that must remain disabled and unchangeable for minors (such as location sharing, unsolicited contact, activation of microphones or cameras without a clear and temporary session-based prompt, or the public display of follower or friend lists) and those settings which can be adapted over time as children grow older and their needs change, provided such changes are guided neutrally and safely.

STATEMENT (Digipeace (Digirauha ry)). Highlights the importance of defining which privacy settings children control and cautions against nudging them towards lowering these settings.

b) Default settings: clarify which of the settings children should have control over depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown). Warns against age verification schemes requiring government-issued IDs, citing disproportionate privacy and security risks for sensitive content access.

We believe that requiring EU residents to submit government issued identification documents for the purpose of age verification, even when accessing adult content, is a highly intrusive and disproportionate solution.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Recommends by-default limitations on others' ability to contact minors or access their data on platforms, reinforcing strong default child privacy controls.

limiting the ability of other users or visitors to communicate with the minor; preventing other users or visitors, whether registered or not, from viewing the minor's personal data collected by or shared on the covered platform, in particular restricting public access to personal dat

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Strongly endorses Article 28(1) guidelines as vital for delivering a secure digital environment for children, supporting effective regulatory enforcement.

Together with the 32 undersigning organisations and experts from across Europe, we strongly support the draft guidelines on Article 28(1) of the Digital Services Act (DSA), which require platforms accessible to minors to ensure a high level of privacy, safety and security.

Feedback DSA (unknown). Draws attention to the need for safeguards for children appearing in family content online, particularly regarding visible consent, privacy, and commercial exploitation.

What safeguards exist for children featured in influencer content (e.g., “mom-fluencers” and family vloggers)?

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Reminds that special attention must be devoted to minors' right to privacy in line with DSA Article 28(1) requirements.

Conformément à l'approche retenue au 1 de l'article 28 du DSA, l'Arcom rappelle qu'une attention particulière doit être portée au respect du droit à la vie privée des mineurs.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Advocates for balanced solutions that protect children online while upholding their privacy, autonomy, and broader human rights.

La CNCDH renouvelle ici sa préoccupation de parvenir à des solutions équilibrées garantissant la sécurité et la sûreté des enfants tout en préservant le respect de leur vie privée et de leur autonomie ainsi que, plus largement, de leurs droits fondamentaux tels qu'ils sont consacrés par la Convention internationale relative aux droits de l'enfant.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Recommends defaulting minors' accounts to maximum privacy, safety, and security, with tailored relaxation of safeguards only when justified by additional assurances.

the default setting must commence with the most restrictive configuration for privacy, safety, and security, until further assurance permits relaxing the safeguards.

1.1.11 Technical Security Measures

The insights within the 'Technical Security Measures' category emphasize a comprehensive approach to protecting minors' privacy, data, and security online through layered technical safeguards. Key themes include minimizing the discoverability of minors' accounts beyond platform boundaries, enforcing default-off settings for sensitive data access (such as geolocation, camera, and microphone), and requiring robust security and privacy for any reporting or authentication systems. Documents highlight the inherent risks of third-party involvement in age verification, advocating for data minimization and immediate purging of sensitive data to mitigate security threats, while noting that such deletion may compromise auditability. Further, there is a call for adherence to standardized frameworks for technical architectures—especially in blockchain contexts—through explicit guidance and mitigation of linkability risks, perhaps using cryptographic tools. Password

security education, mechanisms to prevent cross-platform correlation, and consideration of evolving cybersecurity threats are also stressed as vital elements. Ultimately, technical security must balance privacy, auditability, and practical risks, especially when handling sensitive or identifying data of minors across diverse digital ecosystems.

> *he NMA would like to suggest adding in the section for default settings: "geolocation, microphone, photo access and camera, contact synchronisation as well as all optional tracking features are turned off."* (The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority))
>
> *For every one of these tools, the use of a third-party age verification or age estimation vendor - which is necessary for many website platforms - further vastly increases the security risk because the data being transmitted as part of these processes is being transmitted to and/or retained by additional entities.* (CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.))
>
> *Automatically turn off geolocation, microphone and camera as well as optional tracking features after the session ends, if a minor turns them on.* (TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited))
>
> *Linkability and reversibility risks: even when only hashed or pseudonymised data is stored on-chain, there remains a risk of re-identification, especially when such data can be linked with off-chain datasets or metadata.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))
>
> *If a third-party company acting in bad faith collected biometric faceprints of users, it would be impossible for users to know").* (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))
>
> *Require technical safeguards against token reuse, mandate one-time-use credentials or session-based proofs, and enforce no cross-platform correlation policies.* (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). This document stresses the need for safeguards that limit the external discoverability of minors' accounts and personal information, enhancing online safety and privacy for young users.

> *In addition, we recommend implementing safeguards that extend beyond the platform itself and ensure that minors' accounts and their personal information are not easily discoverable through external channels such as search engines.*

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). It advocates for strict default settings on digital platforms, ensuring that optional tracking functions and access to sensitive device features are turned off by default for minors.

> *he NMA would like to suggest adding in the section for default settings: "geolocation, microphone, photo access and camera, contact synchronisation as well as all optional tracking features are turned off."*

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). Addresses the need for standardized and secure off-chain storage designs in blockchain systems and explores technical measures—like cryptographic proofs—to safeguard against on-chain data linkability and residual privacy risks.

> *The Guidelines could benefit from a more in-depth analysis of the residual risks posed by linkability and recommendations for appropriate safeguards, such as cryptographic commitments or zero-knowledge proofs (ZKPs).*

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Argues against dependence on government or third-party providers for age verification to reduce the security/privacy risks of personal data proliferation, advocating for minimal data exposure.

For every one of these tools, the use of a third-party age verification or age estimation vendor - which is necessary for many website platforms - further vastly increases the security risk because the data being transmitted as part of these processes is being transmitted to and/or retained by additional entities.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Emphasizes the importance of ensuring anonymous and confidential reporting mechanisms to maintain both the safety of children and the privacy of reporters.

We want to add that they should also ensure a high level of privacy and security for those reporting by offering the possibility of anonymous reporting and ensuring confidentiality.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Identifies risks around age authentication, recommending minimization and prompt deletion of sensitive data to mitigate threats, but also notes that deleting such data reduces transparency and auditability.

If information is deleted immediately following verification, then those systems are substantially less auditable because there would be no concrete record of the information

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Recommends technical safeguards against re-authentication and correlation attacks by mandating one-time-use credentials and banning cross-platform linkage for minors.

Require technical safeguards against token reuse, mandate one-time-use credentials or session-based proofs, and enforce no cross-platform correlation policies.

Microsoft response to the European Commission's draft 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 (Microsoft). Suggests that guidelines must explicitly consider cybersecurity threats to minors and the necessary balance between privacy, safety, and technical security.

We also note that the Guidelines, as currently drafted, do not focus on potential cybersecurity risks to minors, which may warrant further consideration, especially to the extent online platforms must weigh up privacy, safety, and security considerations in developing mitigation measures.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Stresses the requirement for strong passwords and user education on secure password management tailored to minors' understanding.

Weiters sollten Minderjährige kindgerecht auf eine sichere Verwahrung ihres Passwortes hingewiesen werden.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Recommends that sensitive features like location, camera, and tracking be switched off automatically after use by minors to reduce persistent risk exposure.

Automatically turn off geolocation, microphone and camera as well as optional tracking features after the session ends, if a minor turns them on.

1.1.12 Blockchain and Decentralised Technologies

This category addresses the unique privacy, data protection, and security challenges presented by blockchain and decentralized technologies, particularly under the lens of EU regulations like the GDPR and DSA. Key

knowledge reflects the complexity of distinguishing personal data in blockchain systems, highlighting that identifiers such as wallet addresses or transaction hashes may or may not constitute personal data depending on contextual factors and potential for re-identification. The insights stress the importance of risk-based, proportionate approaches to defining personal data, advocating for explicit, context-aware guidance to avoid regulatory overreach and support innovation. A significant focus is placed on tailoring Data Protection Impact Assessments (DPIAs) to decentralized environments, addressing the lack of central controllership, the irreversibility of on-chain records, and the need for collaboration across entities. The category also emphasizes the need to recognize and incentivize privacy-preserving technologies and blockchain architectures—like geographic node controls and zk-SNARKs—as best practices for compliance and mitigation of data protection risks. Concrete examples differentiating pseudonymisation from anonymisation in blockchain are encouraged to guide stakeholders in practical compliance.

> *Adan believes the Guidelines would benefit from a more in-depth treatment of the question: what constitutes personal data in blockchain contexts? Blockchain systems, especially public permissionless ones, often rely on cryptographic identifiers (e.g., wallet addresses, transaction hashes, or smart contract interactions) that may not directly identify individuals but could be linked to them through auxiliary data.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *In practice, this means that even pseudonymous identifiers like blockchain addresses or hashed values, may fall within the scope of personal data if they can be linked to a natural person through contextual information.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *For instance, the irreversibility of data recording, the lack of central governance, and the potential for linkability or re-identification of pseudonymous data present unique challenges.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *A balanced interpretation, grounded in technical realities and actual re-identification risk, would support more pragmatic compliance.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *The Guidelines could highlight these as examples of best practice, encouraging privacy-aware architecture design.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *The potential for linking on-chain data to off-chain identities is a critical vector of risk. Even when only hash or pseudonymised data is stored on-chain, re-identification may still be possible through external data correlation or behavioural pattern analysis.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

1.1.13 Miscellaneous

The insights in this category emphasize the importance of maintaining technological neutrality and a principle-based, risk-oriented regulatory approach in privacy, data protection, and security, particularly with respect to innovative technologies like blockchain. The content argues that EU regulations such as the GDPR should not prescribe or favor particular technological solutions, but rather assess whether implementations respect core privacy and security principles. Overly restrictive interpretations—such as limiting public blockchains solely based on public access requirements—may hinder innovation, risk driving technological development outside the EU, and undermine legal coherence. The role of regulatory authorities should be to evaluate compliance with foundational principles, not to choose preferred technology stacks.

> *In light of this, Adan urges the EDPB to reaffirm its commitment to technological neutrality and adopt a principle-based, risk-oriented approach that enables diverse architectural models to co-exist, provided that appropriate safeguards are implemented.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *The role of data protection authorities should not be to determine the appropriateness of a given technological stack, but rather to assess whether a given implementation complies with the GDPR's principles, including data minimisation, purpose limitation, and security.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

> *The GDPR does not prescribe or favour any specific technology, nor does it limit the means by which data processing activities can be carried out, provided that the principles and obligations of the*

> *Regulation are respected.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))
>
> *Limiting their use on the sole basis that public access is not strictly required for personal data processing purposes narrows the regulatory lens and may result in unintended consequences for the European digital economy.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))
>
> *Paragraph 49 of the Guidelines suggests that public blockchains should only be employed if public access to the ledger is necessary for at least one of the purposes of the processing.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))
>
> *The GDPR does not prescribe or favour any specific technology, nor does it limit the means by which data processing activities can be carried out, provided that the principles and obligations of the Regulation are respected.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

1.2 Miscellaneous

A central insight across the sub-categories is the focus on ensuring adaptability and inclusivity within digital policy approaches. Maintaining a diversity of business models is highlighted as essential for promoting innovation, competition, and "user choice in the marketplace," particularly in contexts such as online protection for minors. Complementing this, high-quality, detailed examples in guideline documentation are considered crucial for understanding and effectively applying standards; stakeholders are advised that examples must be both "sufficiently detailed and relevant" to aid practical implementation. Together, these themes reveal a broader emphasis on fairness, balance, and practical clarity in regulatory and best-practice frameworks—ensuring no single approach is unduly favored and that stakeholders are well-supported in interpretation and compliance.

1.2.1 Business Model Diversity

The core knowledge embedded in the 'Business Model Diversity' category is the importance of maintaining a range of business models within the digital sector. The insight emphasizes that regulatory frameworks, particularly those focused on protecting minors online, should be designed to avoid privileging or disadvantaging particular business models. Preserving this diversity is seen as vital for fostering innovation, competition, and user choice in the marketplace.

> *Preserve business model diversity;* (Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance))

1.2.2 Guideline Examples and Development

The 'Guideline Examples and Development' category emphasizes the importance of providing clear, systematically developed examples of good and poor practices in official guidelines. It highlights that while such examples can be beneficial for understanding and implementing the guidelines, those included must be sufficiently detailed and relevant to be truly helpful, especially when illustrating poor practices. The insights suggest a need for more thorough and consistently presented examples throughout the documentation to increase clarity and usefulness for stakeholders.

> *In principle, the provision of examples of good and poor practice is helpful, but some examples, particularly those of poor practice, are not particularly helpful.* (Consultation on the Guidelines on Protection of Minors Online under the Digital Services Act (Association for Computing Machinery (ACM)))
>
> *The examples should be more systematically developed throughout the Guidelines.* (Consultation on the Guidelines on Protection of Minors Online under the Digital Services Act (Association for Computing Machinery (ACM)))

1.3 Age Assurance and Verification

A defining insight across age assurance and verification is the widespread shift away from self-declaration towards robust, privacy-preserving, and proportionate technical standards that harmonize protection for children online across the EU. The need for risk-based, flexible frameworks emerges strongly—more stringent verification for high-risk content, with a spectrum of options for lower-risk services, aiming to avoid intrusive or one-size-fits-all mandates. As one sub-category notes, platforms should "make use of the least intrusive yet effective measures possible" according to their risk profile. Interoperability, harmonization, and clear lines of

responsibility underpin effective implementation, as stakeholders call for consistent yet adaptable solutions that respect both national and EU regulatory diversity. Careful attention is paid to inclusivity and accessibility, demanding multiple, user-appropriate verification avenues to avoid digital exclusion or inadvertent discrimination, particularly for minors lacking conventional ID documents or digital literacy. Transparency and external oversight are considered essential: regular audits, independent evaluations, and mechanisms for user redress help build trust and accountability beyond platform self-assessment. Privacy and data protection remain paramount throughout, with calls for double-blind or data-minimizing solutions and opposition to excessive data collection or profiling. Underlying these strands is a shared commitment to balanced, rights-respecting systems that protect children while upholding user privacy and accessibility. Common threads include the mandate for technological neutrality, proportionality, and collaborative governance, indicating a maturing policy and technical landscape responsive to evolving digital risks and societal values.

1.3.1 Regulatory Standards and Compliance

This category, 'Regulatory Standards and Compliance' under Age Assurance and Verification, encompasses a broad spectrum of legal, technical, and policy considerations relating to protecting minors online in the EU. The insights highlight a strong movement toward harmonized minimum age thresholds (commonly advocating for a 16-year-old minimum for social platforms and 18+ for adult content) until proper protection can be independently verified. There is robust advocacy for mandatory, verifiable age verification and assurance mechanisms—moving beyond self-declaration to more reliable standards, often referencing alignment with bodies like Ofcom, IEEE, or ISO for technical benchmarks, and emphasizing auditability, privacy, and proportionality. Consensus emerges around the need for EU-wide common standards, interoperability, and harmonization, albeit with allowance for national flexibility and respect for existing legislation. Guidance broadly calls for age assurance across all platforms with potential child risk (including unregistered users and specific high-risk features), clarity on acceptable methods, and the avoidance of overreliance on platform self-determination. Yet, some submissions caution against overreach or the imposition of uniform technical mandates without sufficient legal foundation, emphasizing proportionality, privacy, and fundamental rights. Additional recurring themes include due diligence and accountability for external age assurance providers, seamless integration with national digital IDs or wallets, and ensuring that regulation keeps pace with technological evolution while safeguarding the rights of children and users.

> *Adopt European wide age thresholds of minimum 16 years old, at least until there is independent verification that these guidelines (that need further improvement as stated in this document) have been fully implemented and that young people are not being harmed anymore.* (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))
>
> *The guidelines should not mandate a specific age verification method and should align with existing valid verification approaches under EU and national laws.* (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))
>
> *Standards such as IEEE 2089.1 and ISO/IEC 27566-1 offer a path to consistent, measurable and auditable assurance levels* (Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association))
>
> *The Parliament is examining a draft law aiming to secure and regulate the digital space, including the goal to protect children from online pornography through the reinforcement of the ARCOM powers, allowing it to decide, without judicial intervention, the blockage of the websites breaching age verification obligation.* (EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform))
>
> *The threshold COULD potentially be reviewed downwards IF all the guidelines are being adopted and implemented by VLOPs, and have proven to work.* (Policy_demands (unknown))
>
> *The protection of minors cannot depend on the goodwill of profit-driven platforms or the competence of under-resourced institutions. It requires clear obligations, independent oversight, and personal accountability for those who fail our children.* (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Advocates for a European-wide minimum age threshold of 16 for access to platforms with proven harm to child wellbeing, emphasizing that this should remain until guideline effectiveness is independently verified.

Stellungnahmen zum Leitlinienentwurf zum Minderjährigenschutz im Digital Services Act (Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)). Recommends consistent application of age restriction and verification standards to both online shops and physical stores, underscoring the need for unified regulatory expectations.

Für Onlineshops und stationäre Läden müssen einheitliche Altersbeschränkungen bzw.

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). Calls for robust, effective age assurance mechanisms as listed by Ofcom, prohibits exposure to pornographic content before or during age checks, and warns against reliance on self-declaration or inadequate payment-based checks.

Stipulates that pornographic content must not be visible to users before or during the process of completing an age check. Additionally, services must not host or allow content that encourages or directs users to circumvent an age assurance process.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Echoes the call for a 16+ minimum age EU-wide for platforms causing harm to young people's wellbeing, maintaining it until independent verification of guideline effectiveness.

Adopt European wide age thresholds of minimum 16 years old, at least until there is independent verification that these guidelines (that need further improvement as stated in this document) have been fully implemented and that young people are not being harmed anymore.

Response to the European Commission's Consultation on the Draft Guidelines for Article 28 of the Digital Services Act (DSA) (European Commission). Highlights the need for greater clarity in the EU Digital Services Act guidelines regarding the scope and trade-offs of age assurance, particularly the balance of child safety and fundamental rights.

of inherent trade-offs, the guidelines may fall short of effectively balancing children's safety with their rights to privacy, inclusion, participation, and freedom of expression.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Recommends restricting unregistered or unlogged-in users from accessing age-inappropriate content and features, advocating for wider adoption of existing precautionary measures.

Restrict access to age-inappropriate content, i.e., age-restricted content, and features, i.e., chatting or commenting, for accounts that access the service without having logged in or registered.

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). Stresses the importance of clear, robust age verification guidelines for both social media and adult content platforms, and suggests incorporating digital wallet-based age verification in line with EU standards.

Additionally, we would like to underscore the importance of age verification as an effective method for enforcing age restrictions on social media platforms, which currently have a minimum age limit of 13 years, as well as on online platforms offering adult content, products, and services, which have an age limit of 18 years.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Advocates against mandating a specific age verification method, recommending alignment with valid approaches recognized by EU and national laws, and presumption of adequacy for compliant platforms.

The guidelines should not mandate a specific age verification method and should align with existing valid verification approaches under EU and national laws.

Ten recommendations to the European Commission to really protect children online (unknown). Supports an EU-wide minimum age threshold of 16 for platforms causing harm to minors, unless guidelines are demonstrably effective and harm is mitigated.

Adopt European wide age thresholds of 16 years old, at least until there is independent verification that these guidelines (that need further improvement as stated in this document) have been fully implemented and that young people are not being harmed anymore.

Salminen contribution protection of minors (Aalto University). Proposes harmonised age restrictions not for platforms as a whole, but for specific high-risk features, urging the Commission to consider risk-based differentiation.

Instead of imposing access restrictions on all social media platforms, a more effective approach could be to set harmonized age limits for specific features, such as vertical video feed, private messaging, or live stream–many of which are already subject to internal controls by the platforms themselves as shown in this study.

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). Seeks clarification and possible acceptability of self-declaration as an age assurance method, and calls for more transparent rules on its use.

In particular with respect to self-declaration, we believe it would be helpful to clarify whether this method is considered acceptable under any circumstances.

CONCLUSION & POLICY DEMANDS (unknown). Reinforces the push for a 16-year-old minimum age threshold for general platform access, conditional on verified effectiveness of protective measures.

Adopt European wide age thresholds of 16 years old, at least until there is independent verification that the guidelines have been implemented and that no more young people are being harmed.

Ten recommendations to the European Commission to really protect children online (unknown). Demands adoption of a pan-European minimum age threshold of 16 for platforms posing risk to minors, unless harm prevention is proven effective.

Adopt European wide age thresholds of 16 years old, at least until there is independent verification that these guidelines (that need further improvement as stated in this document) have been fully implemented and that young people are not being harmed anymore.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Argues for dedicated, lean regulation on age verification and parental approval, beyond existing DSA guidelines, and recommends EU-US harmonisation efforts.

However, specifically on age assurance, we recommend that instead of addressing age assurance via Guidelines, the EU should issue new lean regulation on age verification and parental approval, which should complement DSA, to effectively close the gap on age verification.

ACT RESPONSE TO THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Association of Commercial Television and Video on Demand in Europe (ACT)). Calls for mandatory, standardised, and accountable age verification for Video Sharing Platforms (VSPs), highlighting current shortcomings and risk-based verification.

Given these shortcomings, we strongly recommend that the Commission prioritise VSPs by adopting mandatory, standardised age verification measures across all such platforms, as they represent the most problematic environment for minors.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Raises the issue of due diligence for platform use of third-party age assurance providers, emphasizing the need for platforms to assess provider effectiveness claims.

Where an online platform uses a third party-provider to carry out age assurance, it is not clear to what extent the online platform needs to conduct due diligence to assess whether the provider in question meets the effectiveness parameters.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Proposes clarifying that age restriction triggers at checkout or delivery for online-restricted products, aligning online and offline verification standards.

Access" to restricted products in Lines 250-253 should refer to the checkout or delivery stage (depending on applicable national or EU laws), not just viewing a product page.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Argues that DSA guidelines should exclude sectoral minimum ages governed by other EU or national laws, keeping the focus on DSA-relevant requirements.

However, in this particular case, the sale of products above a certain age is governed by other sectoral legislation, such as built-in limits for online payment methods. As this falls outside the scope of the DSA, these examples should not be included in the guidelines.

Additional contribution (Collective Shout). Calls for mandatory age verification on all platforms where minors may interact, especially high-risk platforms such as social media, dating, and gaming sites.

We recommend age verification should be used by social media sites, dating apps, any platform that hosts user generated material (in addition to the existing requirement that all video sharing platforms must establish and operate AV), and all platforms where children can connect with other users, especially gaming sites and platforms, as these are routinely used by predators for contacting and grooming children.

Amazon's contribution to the Guidelines on the protection of minors under Article 28 of the Digital Services Act (DSA) (Amazon). Warns against the imposition of new EU-wide baselines that could negate nationally recognized age verification methods, and emphasizes equivalence for online and offline sales.

We believe that the guidelines should not seek to prejudice existing valid means of age verification under EU Member State law.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Stresses that age verification must also apply to adult commercial communications, not just direct content access.

Make it explicit that the requirement for age verification regarding adult content also covers adult commercial communications (ex. gambling content also covers commercial communications about gambling)

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Recommends that age assurance occurs at each session regardless of registration status, and prohibits platforms from suggesting ways to bypass age controls.

Furthermore, to better protect minors by safeguarding them from accessing illegal or dangerous content, for example, using an adult's account or device, it is deemed appropriate to add at the end of paragraph 6.1.3 the provision that, when a website or online platform uses age assurance mechanisms, whether in the case of a registered user (user account) or an unregistered user, the age assurance mechanism must occur at each consultation of the website or specific online platform that disseminates content reserved for adults.

Policy_demands (unknown). Reiterates advocacy for an EU-wide 16-year-old minimum age for access to platforms with demonstrated harm risk, pending proven effectiveness of safeguards.

Adopt European wide age thresholds of 16 years old, at least until there is independent verification that the guidelines have been implemented and that no more young people are being harmed.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Highlights the lack of internationally agreed or government-mandated age verification standards, underlining enforcement challenges and the risk of circumvention.

at present there is no agreed standard for age-verification that is adopted internationally, which means it is impossible to prevent circumvention of Website-Level AV using VPNs.

Yoti_response_on_Article_28__2_.pdf (Yoti). Recommends that only verified age verification (not estimation) should be used for access to high-risk or 18+ services.

Age verification only

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Advises broad interpretation of DSA Article 28(1) to ensure platforms cannot avoid obligations by merely stating age restrictions, and outlines comprehensive age verification needs.

When an online platform grants access to content labeled as "over 18", it should have a certified age verification system in place.

Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act Allwyn submission (Allwyn). Covers compliance with national and EU regulations on age verification and internal best practices to prevent underage access.

Compliance with national legislation on minimum age, internal policies, standards and best practices;

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Emphasizes the foundational role of digital age ratings for controlling age-appropriate access and supports integration flexibility between EU and national age verification systems.

age ratings provide the basis for age-appropriate access.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Urges immediate implementation of mandatory age verification standards with real consequences for all platforms to effectively protect minors.

mmediate (0-3 months): · Age verification for all platforms

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Advocates for clarity and consistency in age assurance guidelines and stresses the importance of aligning with existing national lawful methods.

The guidelines should not mandate a specific age verification method and should align with existing valid verification approaches under EU and national laws.

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). Suggests referencing international standards such as IEEE 2089.1 and ISO/IEC 27566-1 for consistent, auditable age assurance frameworks.

Standards such as IEEE 2089.1 and ISO/IEC 27566-1 offer a path to consistent, measurable and auditable assurance levels

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Reiterates the need to avoid

mandating one-size-fits-all verification methods and encourages alignment with national Member State approaches.

The Guidelines should not demand that a certain age verification method be used and whatever solutions ends up being applied, it should be aligned with the existing verification approaches of EU Member States.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Identifies a gap in current self-determined age requirements on platforms (usually 13), and proposes 16 for social and 18 for adult content.

Requirement: Minimum age 16 for social platforms, 18 for adult content

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Highlights fragmented age verification approaches across the EU and calls for harmonization to reduce regulatory divergence and strengthen protection.

Promote harmonisation at the EU level, especially in light of fragmented national initiatives and diverging interpretations of age assurance standards;

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Proposes mandatory age verification and EU-wide minimum thresholds (16 for social, 18 for adult content), noting platforms self-determine ages currently.

Requirement: Minimum age 16 for social platforms, 18 for adult content

EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform). Describes shift from national to EU-wide regulation for online age verification due to DSA, noting withdrawal of national legislation at the EU's request.

However, on 1st November 2023 the Government announced it is putting the national legislative proposal on age verification on hold and is now putting all efforts into an effective European solution.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Warns about implicit verification mandates and legal obligations that might force platforms to verify all users or censor content for everyone to avoid liability.

We call these bills 'implicit age verification mandates' because, though they might expressly deny requiring age verification, they still force platforms to either impose age verification measures or, worse, to censor whatever content or features deemed 'harmful to minors' for all users-not just young people-in order to avoid liability").

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Calls for greater specificity about mandatory and permissible age verification and estimation methods, especially for high-risk and 18+ content.

Concerning the table in line 297, the first bullet point should make clearer that age verification is mandatory for content and goods which are legally restricted to 18+.

Art. 28 DSA Leitlinien Stellungnahme der Medienanstalten (Medienanstalten). Supports use of established national age assessment methods, including age estimation, for 18+ content like pornography, and opposes blanket EU restrictions on these approaches.

emnach können „age-estimation"-Systeme gemäß der Entschei- dung der KJM auch im Bereich der Pornografie eingesetzt werden, da sie sich als sichere Methoden erwiesen haben, um das Alter von Personen effektiv zu prüfen.

Public consultation on the protection of minors' guidelines under the Digital Services Act (Telefónica S.A). Requests clarification on the interplay between national/EU law and age verification obligations, particularly for services allowing minors under 18.

Further clarification on the application of Union or national laws in determining the use of age verification systems, particularly when the minimum age stipulated by these laws for accessing certain services or products is below 18.

Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown). Argues that a uniform, principle-based framework for age assurance is needed to avoid stigmatizing particular content types or uneven requirements.

We are concerned that prescribing different acceptable age assurance methods based on the type of content or service offered may stigmatise certain sectors, particularly the adult entertainment industry.

Feedback DSA (unknown). Recommends that age verification systems support multiple thresholds (e.g., under 13, under 16), not just a single 18+ standard, to match varied legal regimes.

Age verification systems should support multiple age thresholds (e.g., under 13, under 16), not just a 18+ standard, to reflect varying national restrictions on youth access to certain platforms.

Mastercard Response to the European Commission Public Consultation on DSA protection of minors online (Mastercard). Requests clearer definitions and safeguards for proportionate, data-minimizing and non-intrusive age verification aligned with data protection requirements.

Specifically, clarification on these points would support alignment with the principles of proportionality, data minimisation, and non-intrusiveness detailed in the guidelines and the European Data Protection Board statement on Age Assurance.

euCONSENT ASBL response to Art 28 consultation (euCONSENT ASBL). Endorses building a fast, pan-European age assurance ecosystem based on existing standards, audits, certifications, and protocols for interoperability and trust.

Far from delaying the deployment of a comprehensive EU-wide solution, we believe creating a single pan-European ecosystem, built on audits, international standards, certification and common protocols will be a far faster route to market.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Advocates for mandatory age verification for all video-sharing platforms regardless of size, and for ensuring platforms—not app stores—are accountable for user age checks.

L'Arcom se réjouit que la Commission souligne dans son projet de lignes directrices que la directive sur les services de médias audiovisuels exige que tous les fournisseurs de plateformes de partage de vidéos (Video-Sharing Platforms- VSP ou PPV), même s'ils sont qualifiés de micro ou petites entreprises au sens du RSN, mettent en place et exploitent des systèmes de vérification de l'âge pour les utilisateurs de leurs services en ce qui concerne les contenus susceptibles de nuire au développement physique ou mental des mineurs.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Asserts current age requirements are inconsistent (usually 13), and advocates EU-wide thresholds (16 for social, 18 for adult), and mandatory verification for all platforms.

Requirement: Minimum age 16 for social platforms, 18 for adult content

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Calls for EU Digital Wallet age verification mechanisms to extend beyond high-risk to medium-risk contexts, and for compliance with EU data protection and AI laws.

In Zeile 260 soll lediglich beim Vorliegen von „hohen" Risiken, die nicht mit gelinderen Mitteln als Altersüberprüfungs-Mechanismen verhindert werden können, das EU-Digitale Wallet zum Einsatz kommen.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT

Europe)). Advocates for a pan-European age assurance standard to ensure interoperability and avoid fragmentation, referencing ongoing ETSI work.

While individual countries such as the UK, France, Spain, and Germany have started to develop specifications for age assurance tools, it would be preferable for a European standard to be created to ensure interoperability across the EU.

Additional recommendations and comments on the draft guidelines (Mediahealth for children and youth). Insists on robust, verifiable age checks for access to (especially pornographic) adult content, with clear platform responsibility and enforcement measures.

Age assurance for access to such content must always require robust, verifiable age verification - not mere self-declaration or weak age estimation methods.

Position Paper on the Protection of minors guidelines under the Digital Services Act (InfoCert S.p.A.). Suggests presumptive compliance for providers relying on qualified trusted service providers (QTSPs) in age verification, supporting harmonized implementation across states.

Moreover, introducing a presumption of compliance when a provider relies on a QTSP for age verification would offer a clear, harmonised compliance pathway for market actors, while supporting consistency and trust across Member States.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Recommends linking age verification with checks for legal contractual capacity, particularly in defining spending limits for minors.

Mögliche Maßnahme: im Zusammenhang mit Age Verification auch eine Überprüfung der Geschäftsfähigkeit einführen.

Guidelines to ensure high levels of privacy, safety, and security for minors online (Kaspersky). Proposes expanding the list of age-restricted products/services (e.g., tobacco, energy drinks, violent content) that would require age verification.

With respect to point 6.1.3 ("Determining which age assurance methods to use"), the following categories could be added to the list of products and services subject to minimum age restrictions under Union or national law:

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 (European Commission). Clarifies that platform obligations relate to actual access by minors, not just declarations, and that age checks should factor in national contract laws and guardian consent.

recital 71 of Regulation (EU) 2022/2065 explains that one example of a situation in which a provider of online platform should be aware that some of the recipients of its service are minors is where that provider already processes the personal data of those recipients revealing their age for other purposes, and this reveals that some of those recipients are minors.

Position of Polish Confederation Lewiatan on Commission's consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan). Argues that DSA guidelines, being non-binding, should not impose mandatory age verification or assurance measures.

Having said that, we believe that DSA guidelines are not the place to impose obligatory measures pertaining to age verification or age assurance due to their non-binding nature.

Feedback for 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 (xHamster). Calls for clearer definitions and practical guidance on the distinctions and requirements for age estimation versus age verification, emphasizing reliability and accuracy.

The age verification definition along with the clarification on the difference between age estimation and age verification seem to be contradictory.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Argues against interpreting DSA Article 28 as mandating platform-wide age verification or assurance, cautioning against impacts on privacy and expression rights.

In our perspective, Article 28 should not be interpreted as requiring providers of online platforms to implement age verification or age assurance systems to meet the objectives of ensuring high levels of privacy, safety and security for minors.

Ten recommendations to the European Commission to really protect children online (unknown). Again supports a 16-year-old minimum EU-age threshold for platforms, unless independent verification ensures guideline effectiveness and no ongoing harm.

Adopt European wide age thresholds of 16 years old, at least until there is independent verification that these guidelines (that need further improvement as stated in this document) have been fully implemented and that young people are not being harmed anymore.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Greece proposes a pan-European digital age of majority and binding technical standards for design, recognizing ultimate EU regulatory authority for large platforms.

Greece advanced a set of proposals aimed at establishing a pan-European digital age of majority for social media access and creating binding technical standards for age-appropriate, child-friendly app design.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Stresses explicitly that age verification for adult content also needs to cover related advertising and commercial communications.

Make it explicit that the requirement for age verification regarding adult content also covers adult commercial communications (ex. gambling content also covers commercial communications about gambling)

Joint Statement on Article 28 Guidelines (5Rights Foundation). Calls for adoption of detailed age-appropriate design standards and frameworks (e.g., CWA 18016, IEEE 2089) under the DSA for compliance and best practice.

tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

Input from the ECA to the Guidelines on protection of minors online under the Digital Services Act (European Casino Association (ECA)). Mandates stricter due diligence and business partner verification for platforms containing gambling content to block illegal activity and ads.

By mandating stricter due diligence processes for platforms, including verifying the operators requesting to upload on their online space gambling-related content, the DSA would make it more difficult for illegal gambling operators to use their channels for advertising.

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). Warns against assumptions that age restrictions indicate unsafety, cautioning against misinterpretation of minimum age policies as reflections of inherent service risk.

The text at lines 280-283 seems to incorrectly assume that where an online platform imposes a minimum age requirement below 18, the platform has concluded that its service is not safe or secure for use by minors under that minimum age.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Recommends adding principles of interoperability, consistency, and cross-

legislation compliance to age assurance, and advocates limiting robust age verification to 18+ services until tools mature.

There should also be an explicit adoption of three additional, fundamental age assurance principles: (i) Interoperability; (ii) Consistency; and (iii) Compliance with Other Relevant Laws (including in particular data portability and interoperability of age data and tools in the Digital Markets Act).

On the concept of personal integrity in the german protection of minors (unknown). Notes the obligation for providers to label content with age ratings and highlight interaction risks, with exceptions for smaller or adult-only platforms.

As a result of the amendment of the Youth Protection Act, providers of games or films that make their content available for users digitally on platforms are now also obliged to label them with an age rating and flag up interaction risks if these are to be considered an essential component of the medium.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Supports DSA-aligned adoption and use of global, standards-based, privacy-respecting frameworks for age-appropriate safeguarding of children and vulnerable groups.

IEEE SA aligns with the DSA's call for the development and use of technical standards and goal to foster a safer online environment and posits that age-appropriate design, grounded in ethical, privacy-respecting and standards-based technological frameworks is essential for helping to safeguard not only children but all vulnerable age groups online.

Feedback on the draft Commission guidelines on DSA article 28 (Swedish Agency for the Media). Questions the relevance of age assurance for adults above 18, amid general calls for user-wide protective measures under Article 28.

The Agency is not entirely clear on what is meant with encouraging a general adoption of the measures for the purposes of protecting all users and not just minors, age assurance for example has very little relevance for a user above the age of 18.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Wants to expand platform awareness definition to include external evidence of minor users and extend strict age verification obligations to high-risk platforms, regardless of minimum age.

We recommend expanding the definition of the third scenario (where the provider is otherwise aware that some of the recipients of its services are minors) to include external evidence demonstrating that minors are using the platform or the service.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Again presses for a minimum age of 16 for access to platforms presenting risks, unless fully effective guideline enforcement is proven.

Adopt European wide age thresholds of minimum 16 years old, at least until there is independent verification that these guidelines (that need further improvement as stated in this document) have been fully implemented and that young people are not being harmed anymore.

INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego). Recommends technical regulatory measures for effective age verification on gambling-like mechanisms, with caution around dark patterns and vulnerable consumers.

Con la finalidad de garantizar la efectividad de la prohibición de acceso o activación por personas menores de edad de mecanismos aleatorios de recompensa, el Gobierno, reglamentariamente, a propuesta del departamento que ostente las competencias en materia de protección a las personas consumidoras y juego y del ministerio competente en materia de transformación digital, podrá adoptar

las disposiciones técnicas pertinentes que permitan una verificación de la edad de las personas usuarias de este tipo de funcionalidade

DSA (Protection of Minors) Guidelines (Samsung Electronics). Argues for the harmonization of the legal definition of a minor's age across EU states to reduce compliance complexity and fragmentation.

Additionally, to ensure a harmonised approach, it would be equally important to establish a common definition of a minor's age across all EU Member States.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Germany advocates expanding age verification use to more high-risk contexts, not limited to areas with explicit legal prohibitions or 18+ boundaries.

Die Bundesregierung ist der Ansicht, dass der Einsatz von Altersverifikationen nicht allein auf den Bereich gesetzlicher Verbote sowie auf den vom Anbieter ab 18 Jahren festgelegten Bereich festgelegt werden sollte.

Position du groupe La Poste (La Poste). Highlights the challenge of identifying minor users for targeted advertising restrictions while minimizing extra data collection and allowing time for technical adaptation.

l'interdiction de la publicité ciblée aux mineurs suppose une capacité à identifier l'âge des utilisateurs, sans pour autant collecter de données personnelles supplémentaires.

1.3.2 Risk-Based and Proportionate Approaches

Risk-based and proportionate approaches to age assurance and verification are widely endorsed across the submissions. Key recommendations include adopting flexible, multi-tiered frameworks that match the stringency of age assurance methods to the risk profile of the service, with low-risk services favoring self-declaration or parental attestation, and high-risk platforms (such as those with adult, gambling, or high-interactivity content) requiring robust age verification, often with external oversight. Many stakeholders caution against a one-size-fits-all or overly prescriptive approach, emphasizing the need for accuracy, privacy preservation, and non-intrusiveness—especially to avoid unnecessary data collection and to respect users' fundamental rights. Benchmarks and clear definitions for "high," "medium," and "low" risk categories are broadly called for, as is external oversight to prevent self-assessment abuses. Several responses stress that age assurance should be integrated into a broader safeguarding strategy and not serve as an isolated requirement. There is also a strong push to allow various age assurance methods, provided they meet outcome-based standards, and to encourage providers to implement the least intrusive yet effective measures possible in light of their specific platforms and user base. A recurring theme is the need for transparent guidance on the selection of methods, evaluation of proportionality, implementation frequency, and the recognition of alternative or additional safeguarding measures beyond technical age checks.

We welcome the recognition that age assurance should be implemented in proportion to the risk of the service, taking account of the impact on user privacy, additional rights and freedoms, and whether less far-reaching measures can achieve the same goal. (Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple))

While more robust age assurance methods may be required for high and medium risk services, the Guidelines should explicitly acknowledge self-declaration as a valid and proportionate mitigation measure in low-risk contexts. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

GitHub affirms the approach to age assurance in Section 6, which calls on age assurance measures to be proportionate to risk presented to minors and applied closest to the source of potential harm. (DSA_Article_28_GitHub_Response (GitHub))

The Guidelines' proportionality framework appropriately considers how the purpose, features, and user base of a platform affect the relative risk it presents to minors. (DSA_Article_28_GitHub_Response (GitHub))

Moreover, in its current form, the EU AV App does not support verification for the 13-17 age group, which is an age bracket allowed on some online platforms. (DOT Europe response1 (DOT Europe))

Finally, we feel the need to emphasise the fact that offenders may themselves be minors; therefore, all protection layers must function in an integrated manner. (Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Requests clear criteria and examples—such as a traffic light system—for assessing risk levels and defining age-appropriate measures; highlights vagueness of the current definitions.

In particular, it is not clear what the definition of "medium risk services" should look like in practice.

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Proposes a phased and privacy-preserving rollout of age assurance, starting with low-level, minimally intrusive measures before stricter ones are adopted.

We propose a four-phase rollout allowing for user acclimatization and data-driven adjustments, beginning with privacy-preserving solutions.

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). Recommends aligning proportionate, frictionless, and privacy-preserving age assurance methods with the risk level of platforms as required by the DSA.

Article 28 of the DSA specifically requires online platforms to implement measures that ensure a high level of data protection and safety for minors.

Response to the European Commission's Consultation on the Draft Guidelines for Article 28 of the Digital Services Act (DSA) (European Commission). Advocates for clarity in the use cases that strictly necessitate age verification and warns against oversimplifying risk-based analyses.

In an effort to clarify the appropriate use cases for age verification and age estimation, the EC, however, appears to oversimplify the analysis.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Highlights the need for nuanced risk assessment and robust, risk-appropriate protections, acknowledging ongoing debates about consensus on online minor safety.

The guidelines rightfully point to some of the risks and concerns minors face online, such as cyberbullying, grooming, exposure to illegal or otherwise harmful content, which require robust protection to ensure children can thrive online.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Emphasizes that technical verification alone is not enough and advocates for a broader, integrated approach to age assurance.

we advocate for a more comprehensive and integrated approach to age assurance that extends beyond technical verification.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Supports implementing age assurance in proportion to service risk, recommending parental attestation for low-risk contexts.

We welcome the recognition that age assurance should be implemented in proportion to the risk of the service, taking account of the impact on user privacy, additional rights and freedoms, and whether less far-reaching measures can achieve the same goal.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). Proposes self-declaration as a valid, proportionate age verification method for low-risk services when combined with technical safeguards.

nous souhaitons indiquer que, pour certains services ou types de contenus à faible risque, et à condition qu'elle soit intégrée dans un dispositif technique plus large, la déclaration sur l'honneur de l'utilisateur peut constituer une solution de vérification d'âge valide.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Urges platforms to consider parameters like accuracy, privacy, and non-discrimination before deploying age assurance methods, noting associated risks to fundamental rights.

Before deploying a specific age assurance method, online platforms should consider specific parameters, such as accuracy, reliability, robustness, non-intrusiveness, and non-discrimination to ensure the age assurance technology is effective.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Advocates for age assurance as part of a broader online safety strategy and encourages combining self-declaration with other methods instead of relying solely on verification.

Age assurance should always be viewed as one element within a broader strategy to mitigate risks and support age-appropriate design of online services.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Supports self-declaration for low-risk situations due to its lower impact on fundamental rights, as well as minimal need for sensitive data.

The benefit of this method is that it does not require the provision of any sensitive personal data, such as official identity documents or biometric data.

DOT Europe response1 (DOT Europe). Welcomes recognition of differing risk profiles and techniques but opposes unnecessary barriers to universally suitable services.

We note the Commission's approach to age assurance, recognising different techniques and risk profiles of online platforms and proposing a proportionate understanding of where each methods can be helpful to ensure a high-level of privacy, safety and security.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Critiques mandatory intrusive age verification at the site level, warning it may push users towards riskier, less regulated alternatives.

As access to known and legally compliant sites becomes difficult or invasive, legitimate users of adult websites will move to less regulated platforms, which will proliferate, increasing the risk of minors accessing them.

Yoti_response_on_Article_28__2_.pdf (Yoti). Calls for practical guidance on the frequency and conditions for requiring and reusing age verification, mindful of diverse national approaches.

The guidance is silent on how frequently an age verification - or a re-authentication of a user to re-use a previous age verification - is required.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Recommends recognizing self-declaration as a proportionate option for low-risk features, with robust methods limited to explicit high-risk scenarios.

While more robust age assurance methods may be required for high and medium risk services, the Guidelines should explicitly acknowledge self-declaration as a valid and proportionate mitigation measure in low-risk contexts.

DSA_Article_28_GitHub_Response (GitHub). Affirms the principle that age assurance must be proportionate to the risk posed, especially for inherently low-risk platforms.

GitHub affirms the approach to age assurance in Section 6, which calls on age assurance measures to be proportionate to risk presented to minors and applied closest to the source of potential harm.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Advocates multiple, non-discriminatory, risk-based, and privacy-preserving age assurance methods, and cautions against normalizing intrusive techniques.

While we support a risk-based, privacy-preserving approach, we question the logic that high- risk services should rely on hard identifiers (e.g. facial verification). This may set concerning precedents for normalising potentially intrusive, even privacy-abusive practices in childhood.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Stresses age assurance should be optional in line with proportionality and not perceived as an inevitable requirement in all guideline applications.

In view of the principle of proportionality explained at the beginning of the guidelines, age assurance should be an option, but in the context of the guide- lines' specific provisions, this seems to be an almost inevitable requiremen

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Seeks clearer guidance on applying risk-based age assurance and clarifies which platforms are in scope under Article 28 DSA.

As such, we believe that the risk-based approach should be applied.

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). Recommends an outcome-based, multidimensional standard for assessing effectiveness of age assurance rather than favoring predefined methods.

What matters most is outcome accuracy, not the method used.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Supports age declaration as sufficient for certain platforms, warning that additional technical requirements may unnecessarily impede user access.

For such platforms, an age declaration mechanism should be considered a sufficient safeguard.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Promotes tiered, risk-based age verification, highlighting national discussions on optimizing age assurance guidelines.

To achieve this, access to the platform is forbidden to all minors, whose age is verified when consulting potentially "sensitive" content.

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 (BeSmartOnline! Maltese Safer Internet Centre). Encourages harmonized, robust, and risk-based measures—such as EU digital identity—for high-risk content across the EU.

We fully support the recognition that age verification is a critical enabler of all other protective measures.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Underscores robust age verification for dangerous content and products, deeming self-declaration inappropriate for such cases.

We also support the Commission's view that age verification is appropriate, if not fundamentally necessary, when it comes to dangerous content or products such as alcohol, gambling, dating apps or pornography.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Calls for precise risk benchmarks and external oversight for a tiered, effective approach to age assurance.

a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks.

The European Lotteries' Response to Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act (The European Lotteries). Supports robust, risk-adaptive mechanisms for age assurance, emphasizing alignment with existing national licensing practices.

EL members already operate under stringent national licensing frameworks that mandate effective age verification systems.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Echoes the need to clearly benchmark risk levels and ensure external oversight, linking age assurance to age-appropriate design.

a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Highlights concerns about user burden and recommends limiting persistent age verification to genuinely restricted resources.

requiring publishers to reauthenticate readers' ages every 60 minutes),

Art. 28 DSA Leitlinien Stellungnahme der Medienanstalten (Medienanstalten). Advocates user choice among various age verification systems and sustaining an open competitive landscape.

Insgesamt ist immer entscheidend, dass Nutzerinnen und Nutzer aus einer Auswahl von Altersverifikationssystemen wählen können.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Questions whether age assurance is the most effective or appropriate method to safeguard minors online.

The draft also does not sufficiently show that age assurance is a) the most useful and b) an appropriate way to safeguard children's rights online.

Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance). Welcomes risk-based, context-sensitive requirements but warns against disproportionate reliance on verification mechanisms.

We welcome the draft Guidelines' recognition that age assurance must be risk-based and context-sensitive, and should only apply where a specific feature or content warrants it.

STATEMENT (Digipeace (Digirauha ry)). Urges clear risk benchmarks for different service categories and external oversight for age assurance assessments.

a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks.

Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown). Encourages flexible, privacy-respecting, and technologically neutral approaches, citing advancement of age estimation tools.

We urge the Commission to consider more flexible, privacy respecting approaches to age assurance that uphold the principles of proportionality, technological neutrality, and non-discrimination.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Insists age assurance methods remain accurate and proportionate to risk while acknowledging privacy and access impacts.

We agree with the Commission in that a risk assessment is important to ensure that "any restriction to the exercise of fundamental rights and freedoms is proportionate."

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Notes current guidelines lack clarity in implementation and fail to specify risk category benchmarks for AV/AE systems.

While the guidelines mandate that AV and AE systems must be deployed for high and medium-risk platforms respectively, they provide no clear criteria or systematic scoring mechanisms to define these risk categories.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Welcomes a broad range of alternative and adaptive methods, including age-gating specific features or content.

COFACE welcomes the focus on other alternative measures, as adapting the service for children should always be favoured over excluding them.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Advocates for accepting robust age estimation as an equivalent method to age verification for sensitive adult content, given adequate safeguards.

l'Arcom estime que l'estimation de l'âge pourrait être acceptable, parallèlement à la vérification de l'âge (au sens des lignes directrices), et à condition que les solutions d'estimation de l'âge soient utilisées d'une manière aussi protectrice que la vérification de l'âge.

Microsoft response to the European Commission's draft 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 (Microsoft). Endorses risk-based and proportionate age assurance, with time for innovation in privacy-preserving solutions.

We encourage the Commission to explicitly maintain the principle of a risk-based and proportionate approach to age assurance.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Echoes support for proportionality in age assurance and proposes parental involvement as suitable for lower-risk services.

We welcome the recognition that age assurance should be implemented in proportion to the risk of the service, taking account of the impact on user privacy, additional rights and freedoms, and whether less far-reaching measures can achieve the same goal.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Demands robust age verification with external benchmarks for high-risk services and underscores best practices from harm mitigation.

Establish clear benchmarks and risk categories under which age verification becomes a requirement, building on best practices from threat modelling and harm mitigation.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Suggests clear compliance alternatives for low-risk operators, with stricter requirements reserved only for higher-risk scenarios.

In doing so, it is key that the Europe Commission provides clear and viable ways for low risk online providers to comply with the DSA, without having to resort to age assurance.

Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology). Calls for integrated, standards-based criteria for determining and implementing age assurance in line with risk assessments.

The current text links the appropriateness of an age assurance method to the level of risks associated with a service, as determined through the risk review. However, at present it is unclear what constitutes high risks and medium risks.

Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry). Recognizes age verification's value but insists on a multi-pronged approach with various effective options beyond technical checks.

However, they represent only one of several possible measures and are not sufficient on their own to address all the risks minors face online.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Supports a risk-based framework that values the diversity of practical, privacy-friendly age assurance methods.

Recognize and support diverse, risk-based age assurance methodologies, including the crucial role of interoperable solutions like Credential Manager/Digital Credentials APIs.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Insists on robust age verification as a default across all platforms, with proportional consideration of risk categories.

The Danish Government finds it to be of utmost importance that the guidelines are amended to require availability of robust age verification mechanisms as the default standard for all platforms, presenting a wider range of risk categories to mi- nor

Position of Polish Confederation Lewiatan on Commission’s consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan). Opposes imposing a single technical solution and calls for contextually adapted, phased approaches to age assurance.

We believe that age assurance is critical to creating a safe online environment for minors.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Warns that focusing too heavily on age assurance can neglect addressing the underlying causes of online risk to minors.

By placing a disproportionate emphasis on age assurance as a necessary tool to safeguard minors, the guidelines do not address the root causes of risks encountered by all users, including minors, and instead merely focus on treating their symptoms.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Welcomes risk-based flexibility and argues against holding low-risk or non-child-directed services to the same standards as high-risk platforms.

Indeed services not directed at children - or that pose lower risks - should not be held to the same standards as high-risk services.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Supports effectiveness of access restriction via age but emphasizes not being overly intrusive, favoring graduated solutions.

Cette approche repose sur des dispositifs d'assurance de l'âge plus ou moins efficaces et plus ou moins intrusifs.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Argues that

certain age groups should be barred from economic transactions and online services should not incentivize underage participation.

Certain age groups should not be allowed to enter into economic transactions as they do not yet possess the ability to comprehend spending and money.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Supports robust, interoperable, privacy-preserving age assurance tools including new EU-level solutions.

Vodafone supports the move toward robust, privacy-preserving age assurance mechanisms.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Pushes for age verification barriers around practices prone to cause unintended purchases or addiction among minors.

We recommend ensuring that minors are not exposed to practices that can lead to excessive or unwanted spending or addictive behaviours by setting a minimum age and put such practices behind age verification.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Suggests upstream age signals and contextual safeguards as appropriate risk-based options, reducing friction and promoting efficiency.

Consider such signals, when received and assessed by service providers, as appropriate and proportionate measures under Article 28-especially when combined with contextual safeguards like service-level age estimation mechanisms.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Encourages providers to select proportionate, effective age assurance methods and cautions against unduly broad restrictions.

This would enable providers to choose the most appropriate and proportionate method for their context, provided the method (or combination of methods) meets the standard of effectiveness.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Advocates a fundamental rights-based approach and encourages broader consideration of both children’s rights and technical risks.

We, the undersigned civil society organizations from the fields of child protection/children's rights and internet policy/data protection, call for a differentiated and fundamental rights- based approach to the issue of age verification.

Consultation on the Guidelines on Protection of Minors Online under the Digital Services Act (Association for Computing Machinery (ACM)). Endorses the proportionality principle for all online platform interventions concerning age assurance.

We agree that measures taken by online platform providers should be proportionate.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Supports a risk-adapted and privacy-preserving approach, with acknowledgment of the spectrum of age assurance choices.

Technology Ireland supports a risk-based, interoperable, and privacy-preserving framework for age assurance.

DSA (Protection of Minors) Guidelines (Samsung Electronics). Urges a 'once only' approach to minimize user fatigue and stresses assessing the broader ecosystem when designing risk-based age assurance.

Without this addition of the "once only" principle, users face user fatigue.

1.3.3 Transparency, Oversight, and Governance

The insights under the 'Transparency, Oversight, and Governance' category highlight the critical importance of clear standards, external and independent oversight, and transparent practices for age assurance and verification measures online. Across the documents, there is broad agreement that definitions (such as 'high risk' and 'medium risk'), benchmarks for effectiveness, and processes for auditing or monitoring age assurance systems must be established and consistently applied. Many contributors stress the need for external, rather than self-assessment, oversight and regular, independent evaluations involving different stakeholders (including civil society, technical experts, and, where appropriate, children). Another recurring theme is the emphasis on transparency — not only about how age assurance methods work, but also regarding user redress mechanisms in case of errors, publication of bias mitigation strategies and training data, and clear labelling of age-restricted content or features. Furthermore, the insights stress the importance of minimizing data collection, ensuring accountability (particularly when third-party providers are used), and harmonizing requirements with other regulatory frameworks, including self-regulatory bodies and industry standards. Overall, the call is for an age assurance ecosystem that is not only effective and privacy-preserving but also subject to robust, transparent governance structures.

> *a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks.* (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown))
>
> *Additionally, the assessment should be subject to external oversight, avoiding self-assessment by companies.* (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown))
>
> *an independent monitoring procedure should be established to evaluate the procedures and their security and contribute to the iterative improvement of the system.* (POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab))
>
> *The provider may wish to integrate this mechanism into their internal complaint-handling system under Article 20. See also Section 7.1 of this document.* (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 (European Commission))
>
> *We believe that, when implemented with transparency and accountability, such methods can reliably restrict access by minors while minimising the data collection and processing footprint.* (Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown))
>
> *Service providers may lack direct oversight or control over the inner workings of the age assurance technology used by the third-party age assurance providers, making it challenging to ascertain the presence of biases or discrimination.* (Feedback for 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 (xHamster))

Public consultation on 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 (Coimisiún na Meán). This document recommends enhancing data minimization in age assurance measures and calls for further clarification of risk categorizations and examples of effective age estimation models.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). It highlights the need for regulatory oversight of age estimation technologies, noting the current lack of consistent controls across providers.

> *It remains crucial to bear in mind that, in the absence of any age assurance regulator, or regulation, that any potential acceptance of 'age estimation' as a technology is devoid of controls to ensure a meaningful level of genuine effectiveness from one AV provider to another.*

Yoti_response_on_Article_28__2_.pdf (Yoti). Yoti advocates for regular audit and performance review of age assurance methods, requiring platforms to maintain and submit effectiveness records to regulators.

Platforms should maintain internal records of age assurance system effectiveness (from external and internal providers) risk reviews and rights impact assessments and submit these to regulators annually.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Snap welcomes structured age assurance approaches but urges further clarity and limits on intrusive verification, with consistency and interoperability across laws.

e recommend that: o Age verification should only be required in clear, specific circumstances given its inherently intrusive and exclusionary nature;

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). The USK stresses the importance of transparent age ratings (like IARC), which empower users and are underutilized in current guidelines.

on-consideration of self-regulatory approaches: In particular, age ratings such as those as- signed by the IARC system provide important guidance and increase the level of protection and transparency (awareness and possibility of age-appropriate filtering) by taking into ac- count content and usage risks and providing additional informatio

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). The working group asks for clarified acceptance of different age estimation methods and clearer definitions of risk scenarios.

We also consider it very important that the Commission provides further clarification on what constitutes high-risk and medium-risk scenarios in the context of age assurance.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). This submission clarifies terminology, distinguishing between age assurance, age estimation, and age verification, emphasizing their specific meanings.

Age assurance is an umbrella term for both age verification and age estimation solutions," which is how the term is used in the UK Online Safety Act 2023);

Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown). It supports transparent and accountable deployment of age estimation methods that can protect minors while minimizing data collection.

We believe that, when implemented with transparency and accountability, such methods can reliably restrict access by minors while minimising the data collection and processing footprint.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis calls for transparency in labelling and demands tools be tested for fairness across demographic groups, with disclosure of training data and bias mitigation.

Require tools testing across demographic groups, document model training data sources, and publish bias mitigation strategies.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This contribution highlights the need for clear risk definitions, benchmarks, and external oversight—avoiding reliance on company self-assessment.

a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families

Europe). COFACE emphasizes detailed risk definitions, benchmarks, and the necessity for independent, external oversight of age assurance systems.

Additionally, the assessment should be subject to external oversight, avoiding self-assessment by companies.

euCONSENT ASBL response to Art 28 consultation (euCONSENT ASBL). euCONSENT ASBL urges a pragmatic, stakeholder-driven review of the progress and readiness of interoperable, state-of-the-art age assurance solutions.

We would be pleased to work with all involved, making decisions through consensus across all the relevant stakeholders - as has been our tradition - to achieve the best possible solution based on the state-of-the-art age assurance technologies and interoperability designs in the market today.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Børns Vilkår calls for independent, ongoing impact assessments of age assurance on children's rights, beyond just technical evaluations.

While the guidelines set out important technical criteria for the implementation of age assurance – such as proportionality, accuracy and non-discrimination – they do not sufficiently address the need to evaluate the real-world impact of such systems on children's rights.

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 (European Commission). The Commission's guidelines propose user redress mechanisms for incorrect age assessments and require complaint-handling in platform systems.

Furthermore, providers of online platforms should provide a redress mechanism for users to complain about any incorrect age assessments by the provider (31).

Feedback for 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 (xHamster). xHamster expresses concerns about the accountability and transparency of third-party age assurance providers, particularly regarding bias mitigation.

we have concerns about how service providers, especially those not directly involved in developing their own age assurance methods, can ensure that third-party age assurance providers they utilize effectively mitigate bias and discriminatory outcomes.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document reiterates that effective age assurance demands clearly defined risk categories and mandates independent, external oversight.

Additionally, the assessment should be subject to external oversight, avoiding self-assessment by companies.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). German civil society organizations advocate for independent monitoring to assess the security and effectiveness of age verification, supporting continual improvement.

an independent monitoring procedure should be established to evaluate the procedures and their security and contribute to the iterative improvement of the system.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). It calls for more robust reporting standards for suspected underage accounts to ensure accurate moderation and prevent errors.

The draft asks that all users must be allowed to report suspected underage accounts (743), and we ask that this report should rather be linked to concrete proof (e.g. a post) of the user being too young for the platform.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). PEGI argues that transparent age rating labelling empowers parental and consumer choices, ensuring suitability of gaming content.

The requirement to label the product with the assigned age rating provides parents and consumers with objective, intelligible and reliable information regarding the suitability of a game's content, prior to purchase, or prior to engaging with a game.

1.3.4 Privacy, Security, and Data Protection

The selected documents provide a comprehensive overview of key requirements and challenges in balancing privacy, security, and data protection within age assurance and verification frameworks under the Digital Services Act (DSA). A common position is the need for privacy-preserving, data-minimizing methods that comply with GDPR principles such as data minimization, purpose limitation, privacy by default/design, and user anonymity. Guidelines are urged to require double-blind or third-party verification systems to prevent platforms from accessing sensitive identifying data. Several submissions stress that robust technical standards for age assurance are necessary, with clear boundaries for data use, retention, and deletion, and advocate for innovative privacy-enhancing technological solutions (such as zero-knowledge proofs). Concerns are repeatedly raised about risks posed by identity-based approaches (e.g., uploading government IDs), biometric and behavioral data collection, and reliance on weak proxies such as credit card checks. Contributors recommend that platforms should not be forced to implement intrusive systems in the absence of truly privacy-protective methods, and highlight the danger of normalizing broad collection of personal data, with the attendant risk of data breaches, profiling, and chilling effects on anonymous, lawful internet use. Flexibility and technical neutrality are emphasized—platforms should be able to use diverse, approved tools provided they meet minimum privacy and security standards. Importantly, age credentials and proofs should only be stored as long as necessary and should never be re-used for tracking, profiling, or targeting. Lastly, due diligence responsibilities for platforms (particularly when outsourcing age assurance to third parties) are highlighted, with calls for harmonization with existing GDPR rules and explicit measures for all users, not just minors, in order to maintain both effective protection for children and the fundamental right to privacy for everyone online.

Any age-verification method must integrate privacy-enhancing technologies and comply with the privacy and data protection rules established by the General Data Protection Regulation (GDPR)3 - including the core principles of data minimisation, privacy by design and by default, and purpose limitatio (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

To uphold both user privacy and regulatory intent, we recommend that users should have the choice of an age assurance option which embeds the principles of double-blind architecture by default. (Yoti_response_on_Article_28__2_.pdf (Yoti))

This heightened sensitivity sits atop an already strong European aversion to unnecessary data sharing, reinforced by years of GDPR messaging, and means that measures requiring ID uploads or persistent identifiers prompt immediate avoidance, and rightfully so (Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.))

Criterion 15 requires platforms to provide at least two different methods for proving age. However, to uphold the principle of non-discrimination (Criterion 6), it is critical to establish a real appeal mechanism in case both methods fail (especially due to technical issues). (Contribution Guidelines art 28 DSA (Respect Zone))

the use of age verification systems must not be extended to the point where it fundamentally restricts the anonymous use of lawful services or undermines the right to anonymous communication on the internet. (Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry))

registration needs to consider the prospect of fake accounts and abuse in registration and have mechanisms in place to verify account information. (IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Argues that guidelines should mandate clear assessment criteria, technical

boundaries, and obligations (like data deletion) for age assurance measures, and platforms should not be required to adopt solutions unless privacy and data security can be guaranteed.

They should also point out suitable protective measures and data security standards for the platforms, such as obligations to delete data obtained through age verification or age assurance systems.

Contribution Guidelines art 28 DSA (Respect Zone). Recommends implementation of accurate age verification tailored to age groups, and highlights the ongoing lack of regulatory approval for truly privacy-protective solutions, stressing the need for stringent oversight and transparency.

Respect Zone notes that age verification applications that truly protect personal data are still awaiting regulatory approval, which underscores the need for strict oversight and transparency on the tools used.

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Cautions against requiring identity-based age verification, warning of European resistance to unnecessary data sharing and risks of normalizing persistent identifiers, which can undermine privacy and increase risks of data/identity theft.

Normalizing an online environment where ID or personally identifiable information ("PII") sharing becomes commonplace will undoubtedly create irreversible dangers of potential data and identity theft.

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). Promotes frictionless, reliable age assurance mechanisms using third-party-verified data and underscores the value of leveraging trusted, robust digital identity sources.

Email address age estimation aligns with Ofcom's definition of reliability as it leverages underlying data points rooted in strong digital identity verification, such as those from banks and mortgage lenders.

Response to the European Commission's Consultation on the Draft Guidelines for Article 28 of the Digital Services Act (DSA) (European Commission). Calls for design choices that minimize invasiveness and use of profiling, with privacy-by-default settings, arguing that strong protective outcomes can often be achieved without intensive data collection or estimation.

ecommendation: o The EC should highlight that non-invasive design choices including data :unselected: protection-by-default settings may achieve good-enough protective outcomes without profiling age estimation or age verification methods.

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Asserts platforms hosting explicit content must adopt robust, privacy-preserving age verification, dismissing inadequate self-declaration or weak age-gating as insufficient.

The guidelines appropriately reject self-declaration and inadequate age gates as age assurance methods.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Supports government-level, privacy-protective approaches to age verification, voicing strong opposition to proposals requiring marketplaces to collect sensitive user information.

This is particularly important as we remain deeply concerned about age verification proposals that compromise user privacy by requiring app marketplaces to collect sensitive personal information for all users.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Emphasizes that all age-assurance techniques must comply with GDPR's requirements for privacy enhancement, data minimization, purpose limitation, and privacy by design/default.

Any age-verification method must integrate privacy-enhancing technologies and comply with the privacy and data protection rules established by the General Data Protection Regulation (GDPR)3 -

including the core principles of data minimisation, privacy by design and by default, and purpose limitatio

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Recommends ensuring privacy for age assurance mechanisms in line with GDPR, and accepts age estimation if it meets established privacy, quality, and security benchmarks alongside offering alternative options.

Add age estimation as a viable option to allow access for 18+-content provided that it ensures the same level of security, safety and privacy for minors and meets benchmark for quality for age estimation and if the provider also allows an alternative method.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Proposes that age verification should occur before access to risky content and, to protect user data, suggests third-party verification solutions independent from platforms.

it is suggested that, if online platform providers implement age assurance methods, these must be carried out by third parties that are legally and technically independent of the online platform provider, to ensure that platforms do not come into possession of their users' identifying data, which could be used for purposes unrelated to age verification or, in the worst case, for illegal activities.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Advises against using credit card or ID-document-based methods as primary age assurance mechanisms, citing issues with reliability and risk of misuse by minors.

Using credit card issuance as a proxy for verifying legal age is problematic.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Advocates restricting minors' ability to weaken privacy/safety settings and ensuring age assurance methods minimize or avoid collection of personal data.

Instead, minors should not be able to make account set- tings that might endanger their privacy, safety and security.

Yoti_response_on_Article_28__2_.pdf (Yoti). Recommends double-blind age assurance by default to ensure no personal data or identifiers are revealed, limiting results to simple age confirmation only.

To uphold both user privacy and regulatory intent, we recommend that users should have the choice of an age assurance option which embeds the principles of double-blind architecture by default.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Notes the privacy and security risks of requiring multiple age assurance solutions over time, highlighting the importance of careful implementation to avoid vulnerabilities.

There are potential privacy and security risks with the EU age verification solution, given that platforms have to implement two separate age assurance solutions within a year of each other.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Calls for protective measures applicable to all users, noting particular challenges for effective, foolproof age gating in gaming environments.

This is particularly valuable in gaming environments where effective age gating remains difficult. There is currently no proven, foolproof method of age assurance in games.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Urges harmonization of age assurance obligations with GDPR and existing data protection mechanisms, expressing caution about overextending confidentiality requirements.

We fully support the objective of ensuring that age assurance systems are effective, privacy-preserving, and respectful of fundamental rights - in particular, children's right to privacy as well as the protection of personal data.

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 (BeSmartOnline! Maltese Safer Internet Centre). Recommends mandatory identity verification or dual age checks for children's services and stricter adult-child interaction controls unless adult identity is confirmed.

Require age-gating that limits access to services/platforms designed for children (e.g. games with in-chat features) using identity verification or double-age confirmation for users claiming to be children.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Critiques mandatory online age assurance for diverting resources from proven safety measures and reiterates the importance of data minimization.

age authentication efforts "divert resourcing that could be spent on strategies that are proven to support healthy sexual development").

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Argues age verification should be adaptable to differing content/legal thresholds and only determine if an age barrier has been surpassed, not disclose absolute age.

To ensure that any individual has surpassed (or not) a specific age threshold, a mechanism is required to verify this fact (not necessarily the exact age, but that the threshold has been exceeded). Inevitably, this involves effectively verifying the individual's age (even if the absolute age is not subsequently transmitted).

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Stresses age-related credentials should have strict life-cycle limitations, with prompt automated expiry and prohibition of repurposing for profiling or tracking.

Platforms must ensure that any age-related credentials, tokens, or metadata are not stored longer than strictly necessary, are subject to automated expiry, and cannot be re-purposed for profiling, cross-site tracking, or behavioural targeting.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Proposes not storing age proofs in user accounts and preferring session-based age checks, especially for accessing pornography, while supporting use of digital wallets for age proofs.

concernant le cas d'usage de l'accès à la pornographie, l'Arcom a décidé, dans le cadre de son référentiel technique1, d'adopter une approche hautement protectrice interdisant le stockage des preuves d'âge dans les comptes et exigeant une vérification de l'âge à chaque session, service par service.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Expresses deep concern about age verification schemes that mandate widespread collection of sensitive personal data by app marketplaces.

we remain deeply concerned about age verification proposals that compromise user privacy by requiring app marketplaces to collect sensitive personal information for all users.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Draws attention to platforms' duty to conduct due diligence on third-party age verifiers to ensure both effectiveness and privacy standards are met.

However, unless online platforms need to conduct any form of due diligence whether these promises are indeed factual, online platforms will simply take the age assurance provider's word for it.

Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry). Warns against extending age verification requirements in a way that fundamentally limits anonymous access to lawful services or undermines the right to anonymous communication.

the use of age verification systems must not be extended to the point where it fundamentally restricts the anonymous use of lawful services or undermines the right to anonymous communication on the internet.

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 (European Commission). Notes the rollout of the EU Digital Identity Wallet as a privacy-respecting digital identification solution and highlights risks of inaccurate age assurance.

Member States are currently in the process of providing each of their citizens, residents and businesses an EU Digital Identity Wallet, (24) which will provide a safe, reliable and private means of digital identification within the Un

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Opposes requiring a plurality of age assurance options, pointing out that all methods have privacy, accuracy, or security drawbacks, and highlighting biometric and behavioral data risks.

Obliging service providers to offer a plurality of these age assurance options (lines 301 - 302) glosses over the fact that every solution has serious privacy, accuracy, or security problems.

Overall feedback on the Commissions guidelines on measures to ensure a high level of privacy, safety and security for minors online (ECPAT Sweden). Maintains that age assurance should be a last resort and used only if less intrusive measures cannot achieve the same child protection goals, always respecting children's rights.

If used correctly and as a measure of last resort, age assurance can help create safe and secure online places for children, minimizing exposure to harmful content and with respect for child rights.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Calls for minimum security and privacy standards for age assurance solutions and for the guidelines to explicitly state such criteria while permitting a range of compliant technologies.

while the Guidelines permit alternative interoperable methods to the EU Digital Identity Wallet and EU AV app in Point 274 for Age Verification and Age Assurance, they do not specify what privacy and security criteria such alternatives must meet nor do the Guidelines provide examples of Age Estimation methods that would be considered appropriate (as noted above).

Protecting children online: response to the draft guidance (DIGITALEUROPE). Supports adoption of a risk-based, interoperable, and privacy-preserving framework for age assurance, with recognition of diverse methods.

We support a risk-based, interoperable, and privacy-preserving framework for age assurance.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Highlights the importance of verifying account registrations to prevent abuse, including fake accounts, while keeping security and privacy as central tenets.

registration needs to consider the prospect of fake accounts and abuse in registration and have mechanisms in place to verify account information.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Advocates using zero-knowledge proofs to enable government ID use in age assurance while preserving user anonymity and transmitting only minimal information.

When using government IDs, we believe it is important to emphasize that anonymity, as a central principle of the internet, must be preserved through zero-knowledge proof.

How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition). Suggests online platforms open to minors must use robust, privacy-respecting age verification comparable to EU's official solutions.

The Commission proposes that online platforms accessible to minors should implement robust measures to ensure a high level of safety and privacy.

Consultation on the Guidelines on Protection of Minors Online under the Digital Services Act (Association for Computing Machinery (ACM)). Underlines the risk of excessive data collection through age assurance and insists on strict boundaries: collected data must only serve the purpose of confirming age.

Especially when it comes to age estimation and age verification, data collected about specific individuals should never be used for purposes other than confirming the age of the final content recipient.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Notes the privacy and security risks posed by AI and chatbots in children's digital spaces and calls for more explicit protective measures in the guidelines.

AI practices and chatbots can pose significant risks to children's privacy, safety and security.

DSA Guidelines for Protection of Minors Additional Submission EuroISPA FINAL (EuroISPA). Emphasizes allowing continued use of proven, effective, privacy-compliant age assurance methods and the importance of protecting online anonymity.

It is important to recognize that various age verification and assurance methods already in use have demonstrated effectiveness, accuracy, and reliability.

Position du groupe La Poste (La Poste). Notes France's ARCOM has adopted strict security and confidentiality standards for age verification systems, including prohibiting sharing or re-use of age proofs between users.

Il est notamment précisé que ces systèmes ne doivent en aucun cas permettre le partage ou la réutilisation des preuves d'âge entre utilisateurs, afin de limiter les risques de fraude ou de contournement.

1.3.5 Inclusivity, Accessibility, and Fairness

The documents in this category collectively emphasize the need for age assurance and verification systems that prioritize inclusivity, accessibility, and fairness for minors. A major concern is the risk of digital exclusion, particularly for vulnerable groups such as children without identity documents, refugees, or individuals with limited digital literacy. Many documents stress the importance of offering multiple, accessible methods for age verification, rather than relying solely on government IDs or inflexible approaches that may inadvertently discriminate or marginalize certain users. There is a strong call for age assurance methods to minimize bias, promote equal access, and cater to the diverse needs and abilities of the child population, including those with disabilities. Some insights also warn against the unintended consequences of overly strict or technical approaches, such as erecting digital barriers that limit access to information, or neglecting the nuances between different age groups. The importance of balancing child safety, rights to privacy, and participation is highlighted, alongside the need for transparent, age-appropriate processes. Overall, the insights advocate for an effective, rights-respecting approach that actively addresses discrimination and exclusion while maintaining

strong child protection standards. Platforms are encouraged to consider alternatives to ID-based systems, implement age-appropriate design, and provide user choice and appeals in age verification processes.

> *By appearing to promote ID-based verification above other techniques, the guidelines risk excluding citizens, particularly children, who do not possess documents or cannot safely share them.* (Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association))
>
> *We consider the sole use of government IDs for the purpose of age verification to be critical, as this would exclude numerous groups of people from the process, e.g., children under the age of 16, who are currently not required to carry ID, refugees or persons without valid residence status, and stateless persons.* (POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab))
>
> *We consider it important to ensure that different methods of age assurance are provided by the platform, to enable all children to access these methods regardless of age, capacities or disabilities.* (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))
>
> *Furthermore, recognising that age assurance should be aligned with principles of age-appropriate design.* (SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands))
>
> *Alternative, inclusive methods should be explored.* (Feedback DSA (unknown))
>
> *Discrimination and exclusion mechanisms must be considered and prevented.* (POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). This document calls for more comprehensive action to prevent discrimination in AI-based age estimation, highlighting that existing methods cannot guarantee non-discrimination.

> *As none of the existing age estimation methods guarantee that discrimination will be ruled out with certainty, we cannot endorse them at this time.*

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). It promotes flexible, inclusive age assurance solutions that provide users with different options for verifying age, aiming for fairness and high accessibility.

> *Additionally, businesses should empower their users with optionality.*

Response to the European Commission's Consultation on the Draft Guidelines for Article 28 of the Digital Services Act (DSA) (European Commission). The response outlines the need to recognize and manage trade-offs between child safety and fundamental rights such as inclusion and participation within age assurance regulations.

> *ards, and a recognition of inherent trade-offs, the guidelines may fall short of effectively balancing children's safety with their rights to privacy, inclusion, participation, and freedom of expression.*

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Recommends that platforms offer at least two age verification or estimation methods and provide alternatives for those unable or unwilling to use specific methods.

> *At least an alternative should be provided to users who cannot or do not wish to use a specific method of age assurance.*

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU)

2022/2065 (Bris). Highlights concerns about digital exclusion from the EU digital wallet for children and urges platforms to assess the unintended impacts of age assurance on children's rights.

This brings with it unintended risks of exclusion, especially considering that the digital and technical conditions vary across EU member states.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Supports the principle that minors should have access to platforms unless specifically restricted, and warns against the overreliance on age assurance at the expense of inclusive service design.

We support the Commission's clarification that platforms are considered accessible to minors unless specific measures are in place to exclude them.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Critiques the lack of an age-differentiated approach in the guidelines and notes the risk of focusing protections only on the youngest users.

In particular, a comprehensive age-differentiated approach is missing.

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). Warns that prioritizing ID-based verification may exclude children without documents, and advocates for estimation techniques that improve accessibility and privacy.

By appearing to promote ID-based verification above other techniques, the guidelines risk excluding citizens, particularly children, who do not possess documents or cannot safely share them.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Argues that age assurance practices should align with age-appropriate design, ensuring accessibility for all children.

Furthermore, recognising that age assurance should be aligned with principles of age-appropriate design.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Warns that age authentication can act as an exclusionary barrier, especially for marginalized groups, and highlights the resulting risks of digital divides and restricted access to information.

Age authentication processes act like a virtual "wall" interposed between readers and the content and resources they hope to access.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Emphasizes the importance of effective deterrents to underage registration while balancing respect for children's rights and curiosity.

Deploy effective deterrents: When designing measures to deter minors from lying about their age, ensure that such deterrents are effective, e.g. requiring for a parent's e-mail address or phone number to confirm age of minor

Feedback DSA (unknown). Advocates for age verification systems that do not reinforce digital exclusion, particularly for vulnerable and underserved groups, and calls for more inclusive alternatives.

Age verification systems must not reinforce digital exclusion, particularly for vulnerable groups like migrants, refugees, low-income users, or those lacking access to documentation or limited digital literacy.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). Objects to treating all minors as a homogenous group and stresses the different developmental and safety needs of younger children versus teenagers.

Firstly, we are concerned that the guidelines, as currently drafted, appear to regard under 18s as a homogenous group.

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 (European Commission). Recommends registration and authentication processes for minors be accessible, transparent, and prioritize verified, age-appropriate contacts.

Registration or authentication may influence whether and how minors are able to access a given service in a safe, age-appropriate and rights-preserving way.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Suggests that registration for minors should be technically and linguistically accessible, with clear, child-friendly communication and mental health safeguards.

Greece emphasizes that registration must not only be technically accessible but must also incorporate clear communication in child-friendly formats, such as audiovisual pop-ups, to explain both benefits and risks.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Highlights the use of age ratings and parental controls to ensure age-appropriate content and informed decision-making for minors and their families.

Parents and guardians can use Epic's Parental Controls to set content age rating limits based on their family's preferences.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Calls for consistency in age assurance standards across similar online platforms to ensure fairness and prevent discrimination.

Consistency ensures a clear, fair, non-discriminatory level playing field for all users and online platforms, and is already implied by the other age assurance principles.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Argues that age restrictions should be raised for social media to protect minors' mental and cognitive health, as current limitations are insufficient.

Om mentale gezondheid en cognitieve ontwikkeling te beschermen is dit te laag.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Recommends using age assurance to enable inclusive, age-appropriate design for children and ensuring multiple accessible methods are available for all children.

We consider it important to ensure that different methods of age assurance are provided by the platform, to enable all children to access these methods regardless of age, capacities or disabilities.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Warns against sole reliance on government IDs and urges diverse, accessible verification methods, including vouching systems, to avoid excluding marginalized children.

We consider the sole use of government IDs for the purpose of age verification to be critical, as this would exclude numerous groups of people from the process, e.g., children under the age of 16, who are currently not required to carry ID, refugees or persons without valid residence status, and stateless persons.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). Advocates for nuanced, non-exclusionary approaches to age assurance, ensuring minors without documentation are not left out of knowledge-sharing opportunities online.

As a Q&A-platform, we have already restricted underage users from entering spaces considered age inappropriate, such as highly sexualised content, as suggested by the Commission (211). However, we believe that minors should not be fully excluded from contact with adult users online as they provide the younger generation with insights and assistance and vice versa.

Position du groupe La Poste (La Poste). Calls for equality in age verification across online and physical sales channels to ensure fair access to age-restricted goods and services.

Tout service ou produit interdit aux mineurs de moins de 18 ans - qu'il s'agisse de contenus numériques ou de biens tels que le tabac ou l'alcool - doit faire l'objet d'une vérification d'âge systématique, quel que soit le canal de distribution.

1.3.6 Technical Methods and Innovations

The category 'Technical Methods and Innovations' in Age Assurance and Verification is marked by a strong emphasis on a diverse, flexible, and privacy-respecting toolkit of technical solutions. Stakeholders call for clear guidelines on the accuracy, reliability, and benchmarking of methods like AI-based age estimation, document-based verification with liveness checks, device-level controls, and privacy-enhancing technologies such as zero-knowledge proofs, double-blind architectures, and cryptographic tokens. There is broad support for technology-neutral, harmonized solutions with interoperable digital credentials, and the adoption of innovative approaches (e.g., email-based age estimation, PIN codes for shared devices, and operating system-level assurance) that minimize data sharing and maximize user choice. The need to balance effectiveness, user-friendliness, and privacy is recurrent, with recommendations for layered or multi-method verification depending on risk, as well as regular evaluation and adaptation of technical standards to maintain high levels of child safety online. A representative tension runs through many insights: ensuring robust verification often risks increased intrusiveness, so privacy-by-design is highlighted. Many contributors urge that any single method not be mandated; rather, multiple secure, user-selectable solutions should be recognized. There is also recognition of the limitations of well-known approaches (such as credit card verification or inadequate AI estimation) and calls for robust evidence before deployment of new edicts. Innovations such as device-based verification, digital wallets, and double-verification architectures suggest a maturing field responding both to regulatory frameworks (like eIDAS2) and evolving digital risks.

This could include extending current digital wallets and credential infrastructure, as well as the introduction of interoperable digital wallets that are platform-neutral and open-source zero-knowledge proof technologies, building on existing age-assurance measures. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

In terms of accuracy we would suggest that there should be minimum requirements for liveness detection, such as reference to NIST2 certification for liveness. (Yoti_response_on_Article_28__2_.pdf (Yoti))

Snap strongly supports the inclusion of a wide range of Age Assurance methods in the Guidelines. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

app-based age verification methods are the least preferred option among the currently available methods. (Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown))

If insufficiently accurate, reliable, and robust age estimation methods remain available, platforms will eventually resort to them in order to keep the access barriers to their services as low as possible. (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 Feedback (Gesellschaft für Freiheitsrechte e.V.))

Allow FIDO-anchored, pseudonymous age attestations combinable with wallet credentials. (Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Emphasizes the need for guidelines to set minimum standards and examples of good practice regarding the accuracy and reliability of AI-based age estimation methods.

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Recommends methods such as randomized A/B testing for phased age verification rollout, and emphasizes device-level and privacy-preserving controls, including cryptographic tokens and pseudonymous attestations.

In Phase 2, European traffic could be randomly split between "control" (status quo) and "treatment" cohorts that successively add soft-gate checks, the EU age verification solution, and finally, the EUDI.

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). Advocates for email address-based age estimation as a frictionless, privacy-friendly, and effective method for compliance with global age-restriction laws.

Age estimation using an email address can help businesses comply with global legislative requirements, such as the Online Safety Act (UK), Digital Services Act (EU), various pieces of state legislation across the US and numerous other domestic and international laws related to the sale of age-restricted products such as alcohol and tobacco.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Urges incentivization of Privacy Enhancing Technologies (PETs) to ensure age assurance solutions are privacy-preserving and minimize personal data use.

PETs can play a crucial role in age assurance by enabling the verification of a user's age without requiring access to excessive personal data, thereby upholding privacy and data minimisation principles.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Supports harmonized, transitional technical solutions for age-verification, including open-source zero-knowledge proofs and interoperable digital wallets.

This could include extending current digital wallets and credential infrastructure, as well as the introduction of interoperable digital wallets that are platform-neutral and open-source zero-knowledge proof technologies, building on existing age-assurance measures.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Advises taking a technology-neutral approach to age verification, recognizing that both 'age estimation' and traditional verification can be equally effective depending on the technology and purpose.

The draft guidelines differentiate between "age verification" and "age estimation" as different methods applicable for different purposes.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Recommends development and adoption of standardized technical specifications for age verification in digital services.

Yoti_response_on_Article_28__2_.pdf (Yoti). Suggests setting minimum technical requirements for liveness detection and multilayered document-based age verification, including face matching and anti-injection detection.

In terms of accuracy we would suggest that there should be minimum requirements for liveness detection, such as reference to NIST2 certification for liveness.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Calls for an explicit recognition of a wide range of age assurance methods including age inference models, and clarification on measurement and benchmarking accuracy.

Snap strongly supports the inclusion of a wide range of Age Assurance methods in the Guidelines.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Suggests EU Digital Identity should be one among multiple age verification options, with recognition of eIDAS2 limitations.

The EU Digital Identity should be considered one of multiple age verification options, limited by the scope of eIDAS2 Regulation.

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). Recommends clarifying requirements for double-blind architectures in age verification, noting differences in national mandates.

The document fails to state whether double-blind architectures are required, optional or unnecessary.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Supports considering EU Digital Identity as one of several age verification tools within the eIDAS Regulation.

Within the scope of the elDAS Regulation, EU Digital Identity should be considered one of the multiple age verification tools.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Advocates for user choice in secure age verification methods rather than a single mandated solution, to enhance privacy and adoption.

To this end, in order to facilitate user adoption while respecting their privacy, it seems important not to 'impose' a verification method such as mandatory ID verification, but rather to offer an interface providing several secure solutions (such as double anonymity) from which users can choose.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Stresses the importance of integrating age verification and child protection into service design, applying only where risk warrants it.

The second core dimension is the integration of protection into the very design of the service. This applies first and foremost to age verification.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Presents skepticism about common methods such as credit card verification and raises concerns about biometric and identity-spoofing risks.

See Free Speech Coalition, Inc. v. Rokita, 738 F. Supp. 3d 1041 n.21 (S.D. Ind. 2024) ("credit card verification is not effective at ensuring a user is over the age of 18").

Art. 28 DSA Leitlinien Stellungnahme der Medienanstalten (Medienanstalten). Urges that reliable age estimation systems, when paired with safeguards, be deemed valid even for adult content under the DSA.

Die Medienanstalten fordern die EU-Kommission auf, die Leitli- nien dahingehend zu ändern, dass auch Systeme der „age-esti- mation“ zur Feststellung der Volljährigkeit als geeignet bewertet werden, sofern durch Sicherheitspuffer ein hoher Zuverlässig- keitsgrad erreicht wird und alternative Methoden durch die On- line-Plattform bereitgestellt werden.

Response to the Commission Guidelines Pursuant to Article 28(4) of the Digital Services Act (unknown). Promotes privacy-preserving age estimation technologies like the 'challenge age' approach and recommends device-level assurance while warning against standardizing app-based verification.

Alternative, privacy preserving methods such as age estimation technologies, particularly those that integrate a "challenge age" approach (as recognised by Ofcom under the UK Online Safety Act), can offer effective and proportionate safeguards without compromising fundamental rights.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Calls for minimum technical standards, redress flows for errors, and anti-circumvention features to ensure age assurance tools are accurate and effective.

Define minimum accuracy thresholds and performance metrics to ensure platforms are not using ineffective or biased tools.

Mastercard Response to the European Commission Public Consultation on DSA protection of minors online (Mastercard). Argues for official endorsement and recognition of card-based age verification methods leveraging secure payment infrastructure.

Card-based age verification, leveraging existing secure payment infrastructure, represents a robust, reliable, and user-friendly solution deserving clear endorsement in the Commission's guidelines.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Distinguishes between in-house and third-party age estimation methods, raising concerns about guidance, benchmarking, and data collection in third-party solutions.

Crucially, VLOPs and VLOSEs may have enough data on a portion of their users to be able to make an inference about their age with a high enough level of accuracy and without needing to collect additional data (DSA Art. 28(3). For smaller platforms and new users, however, - as outlined in the section above - the lack of guidance and benchmarking when it comes to the accuracy of third-party solutions raises important concerns regarding additional data collection and low accuracy rates.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Suggests that the age verification framework should explicitly include and standardize Credential Manager/Digital Credentials APIs for interoperability.

These APIs are the essential plumbing that will enable a truly interoperable, user-friendly and innovative age verification ecosystem across the European Union.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Calls for clear delineation and limitation of age estimation methods, advocating for minimal data use when applying such procedures.

Diese Verfahren sollten so datensparsam wie möglich ausgeführt werden.

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 (European Commission). States that providers should assess the effectiveness, especially the accuracy, of any age verification or estimation method before implementation.

Before considering whether to put in place a specific age verification or estimation method, providers of online platforms accessible to minors should consider the following features of that method:

Feedback for 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 (xHamster). Recommends assessing appropriateness and proportionality of age assurance measures, highlighting device-based age assurance as a less intrusive, effective alternative.

Our position is that site-level age verification is not proportionate, given that a less intrusive measure has already been developed, it is easier to implement and actually effective. This is device-based age assurance.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Describes national initiatives and the broader policy objective of implementing effective online age verification to protect minors.

initiatives such as the KidsWallet Application, and the non-paper recently presented by Greece at the Council of the EU in the beginning of June 2025 serve as important milestones for our policy positions, namely the need for effective age verification online,

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Argues for accepting effective age estimation technologies—including image recognition—as valid for adult content, provided alternatives are also available.

The draft guidelines differentiate between "age verification" and "age estimation" as different methods applicable for different purposes.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Supports more technical measures, including further age verification, expecting a wider policy package for online child protection.

We welcome any wider package of measures on child online protection due later in the year, including further technical proposals on age verification & a review of the impact of social media on children's mental health.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Recommends robust age verification and specifically promotes ID wallet-based solutions for enforcement and transparency.

Robust age verification is also necessary to ensure these protections are activated appropriately (Lines 383-413).

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Champions making more than one age assurance method available and describes whole-system approaches including parental consent flows.

Epic agrees with the draft guidelines that platforms "should always make more than one age assurance method available."

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Strongly supports broad inclusion of various age assurance methods and calls for clear accuracy measurement and validation in the guidelines.

Snap strongly supports the inclusion of a wide range of Age Assurance methods in the Guidelines.

Consultation Response from Barnevakten, Norway - Regarding Article 28 of the EU Commission's Digital Services Act (DSA) (Barnevakten Foundation). Acknowledges current age verification as insufficient, supporting estimated age in some cases and advocating for layered, risk-appropriate assurance.

Barnevakten supports the Commission's assessment that current age verification is insufficient for certain online services, and that it is not enough that children simply enter a birthdate when creating a social media account

DSA (Protection of Minors) Guidelines (Samsung Electronics). Proposes a practical age assurance method for shared devices: the use of over-18 PIN code checks, tailored to smart televisions.

As a result, SE implements a more effective age assurance solution to ensure minors do not access higher risk content (information): an "over 18 PIN code check."

Position du groupe La Poste (La Poste). Suggests implementing double-anonymity and zero-knowledge proof mechanisms to guarantee user privacy during age verification.

> *Les solutions techniques mises en œuvre doivent impérativement intégrer des mécanismes de double anonymat et de preuve à divulgation nulle de connaissance (zero-knowledge proof).*

1.3.7 Implementation and Ecosystem

The category "Age Assurance and Verification >> Implementation and Ecosystem" encompasses a complex and multi-layered set of insights focused on how age assurance systems and policies can be effectively, fairly, and securely deployed across the EU digital ecosystem. A strongly recurring theme is the need for harmonization, interoperable solutions, and the avoidance of fragmented or duplicative approaches—whether at the platform, app store, or device level. Many stakeholders recommend phased, real-world pilots (often leveraging EU digital wallet infrastructure), while emphasizing flexibility so that new solutions complement rather than displace existing private sector options or innovations. Key operational challenges discussed include funding mechanisms, cross-platform/cross-service interoperability, privacy, and the technical or financial burden on smaller actors. There is significant advocacy for collaboration at the Member State and EU level to ensure consistent standards, alongside clear calls for clarity on responsibilities (app store vs. platform vs. device manufacturer), and for streamlining checks while preventing repeated or overly-intrusive verification. Some contributors underscore the importance of rapid, adaptive, and risk-based deployment, while cautioning that rushed or overly prescriptive approaches could compromise security or market competition. Overall, the insights stress the importance of a multi-stakeholder ecosystem with clear, consistent, and practical implementation guidelines that maximize child safety and user rights.

> *CIPL also considers it important, in addition to establishing a common risk taxonomy framework for age assurance, to work towards further standardisation, such as through a centralised interoperable age assurance solution that streamlines the process and reduces the burden of repeated checks across multiple services for platforms and users.* (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))

> *The proposed public sector EU AV App must not displace or preclude private sector suppliers and innovation.* (Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association))

> *Mandatory - Currently the API is positioned as an optional mechanism. We believe there are good reasons for the Guidelines to mandate online platforms to offer users the choice to share age assurance credentials via the API to ensure a level playing field across services and ensure a sufficient critical mass of users with credentials.* (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

> *This clarification will help ensure that age assurance methods are applied not only for exclusion but also for creating positive, developmentally appropriate online experiences.* (Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus))

> *This approach would reach more devices than an app store authentication requirement-indeed, it may be overinclusive because so many IoT devices are now Internet-enabled-but it otherwise suffers from all of the same problems.* (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

> *It must be ensured that all digital offerings, including non-profit offerings, can use and finance the system.* (POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab))

> **Contribution Guidelines art 28 DSA (Respect Zone).** Argues for strict access controls on platforms for minors, ensuring only legitimate adult access, and requiring service providers to confirm users' age groups align with their intended services.

> **Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.).** Proposes a phased, pilot-driven roadmap for deploying age assurance, advocating for real-life testing and eventual transition to robust, wallet-grade age verification after key metrics are met.

Build a staggered implementation roadmap Phase 1: soft-level age-assurance (e-mail/SMS, PSD2, Apple /Google wallet ping) plus parental signals, backed by an EU bad-actor reporting hotline with rapid DNS blocks; no hard ID.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Calls for a centralized, interoperable age assurance solution to prevent repeated checks and ensure efficiency, with attention to privacy, security, competition, and liability.

CIPL also considers it important, in addition to establishing a common risk taxonomy framework for age assurance, to work towards further standardisation, such as through a centralised interoperable age assurance solution that streamlines the process and reduces the burden of repeated checks across multiple services for platforms and users.

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). Recommends further centralization of age assurance tools and explicit support for implementing a mini wallet approach across Member States.

That said, we believe the guidelines could take a more centralized approach regarding these tools.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Details Apple's enhancements for age-appropriate controls and verification, highlighting app ratings, child accounts, and parental controls in compliance with DSA.

We are also taking additional steps to support age- appropriate browsing on the App Store, updating our age ratings and product pages to provide greater insight into the apps that children seek to download.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Suggests aligning age verification at the app store or OS level, utilizing pre-existing device ecosystem signals to platforms.

Many app stores and OS have existing processes in place to collect age.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Urges Member State cooperation for consistent age-assurance requirements to maintain Single Market integrity.

CCIA Europe further believes the Commission should promote close collaboration between Member States and their national authorities when discussing age-assurance requirements, with a view to ensuring that different national measures do not undermine the integrity of the Single Market.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Advocates for industry-wide, EU-level solutions due to the scale of adult content online, stressing that no single regulator can manage age-inappropriate material alone.

The Importance of an Industry-Wide Concerted Solution at EU Level and Beyond.

Yoti_response_on_Article_28__2_.pdf (Yoti). Argues for technological neutrality and support for private sector age assurance solutions, encouraging fair competition and consumer choice.

The Commission has emphasized openness to private sector solutions, as long as they meet equivalent standards (especially for privacy, data protection, and effectiveness).

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Supports mandating APIs for age assurance credential sharing, efficient funding, and uniform application of assurance across platforms.

Mandatory - Currently the API is positioned as an optional mechanism. We believe there are good reasons for the Guidelines to mandate online platforms to offer users the choice to share age assurance credentials via the API to ensure a level playing field across services and ensure a sufficient critical mass of users with credentials.

Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children). Emphasizes that effective age assurance must be a shared responsibility extending beyond platforms to include app store and device ecosystem actors.

Highly effective age assurance is a shared responsibility. The proposed guidelines for online platforms about age assurance are appropriate but insufficient, standing alone, without similar responsibilities imposed on app store operators, OS developers, and device manufacturers.

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). Warns that the public EU AV App should integrate private providers and not crowd out market innovation, supporting cross-sector interoperability.

The proposed public sector EU AV App must not displace or preclude private sector suppliers and innovation.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Advocates for an industry-wide approach, possibly including app store integration, and minimizing redundant verification layers.

Further on the age assurance methods, we believe this is an industry wide effort, meaning all actors in the ecosystem should participate.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Welcomes harmonized age assessment solutions such as European digital wallets as essential for effective protective measures for minors.

Concerning age verification, we welcome the explicit recognition that this measure is essential, if not a prerequisite, to the effectiveness of any other protective measure.

Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus). Suggests restructuring guideline sections to clarify the primary purposes and logical sequence for age assurance implementation.

Additionally, we propose elaborating on the three core purposes of age assurance to help platforms understand and adopt appropriate approaches:

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Highlights burdens for startups and smaller actors, pointing out the reliance on third-party age authentication providers and possible negative user behavior outcomes.

no startup will create their own age-verification system, and will instead rely on third-party providers.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Cautions against rushing an EU-wide age verification solution, raising concerns about the security, reliability, and usability given limited development time.

We are also concerned about the promotion of an EU age verification solution to facilitate hard age checks ahead of the broader roll-out of the EU Digital Identity Wallet, expected by the end of 2026.

euCONSENT ASBL response to Art 28 consultation (euCONSENT ASBL). Recommends considering faster, already available interoperable solutions like AgeAware, instead of waiting for prolonged rollout of a new EU AV App.

We believe AgeAware could deliver protections across the EU much more quickly.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom).

Commends ambitious verification guidelines and urges swift implementation, recognizing the 'mini wallet' as the standard or baseline solution.

L'Arcom prend également bonne note de la recommandation d'utiliser le mini wallet (NDLR : solution transitoire de vérification de l'âge qui doit être mise à disposition des États membres par la Commission) en tant que solution naturelle que les plateformes disponibles en UE devraient adopter, et qui constituera la norme vis à vis de laquelle tout autre solution technique devra être comparée ou alignée, si elle est préférée au mini wallet.

Microsoft response to the European Commission's draft 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 (Microsoft). Asserts that age verification should be part of a holistic set of DSA measures, not a standalone solution.

We also note that, while we welcome harmonized efforts being undertaken at EU level, age verification should not be pursued in isolation nor considered a comprehensive solution in and of itself.

Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry). Advocates treating new age verification options as supplements rather than replacements, maintaining plurality in solutions.

New options such as age verification apps and digital identity wallets should be seen as additional options and not as solutions that necessarily replace existing ones.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Argues that responsibility for age assurance should lie primarily at the platform level, with recognition that the greatest risk occurs within apps.

Age assurance solely at an app store level is a flawed approach because it places the responsibility at the wrong point.

Position Paper on the Protection of minors guidelines under the Digital Services Act (InfoCert S.p.A.). Promotes leveraging existing legal frameworks and tech for the rapid deployment of the EU AV App as an interim measure before deploying the full EUDI Wallet.

n this regard, the possibility of adopting a short- term solution, such as the EU Age Verification application currently under development, represents an important opportunity to safeguard minors' rights ahead of the full-scale deployment of the EUDI Wallet.

Feedback for 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 (xHamster). Recommends referencing pre-approved age verification providers to reduce compliance burdens, and stresses the value of centralized verification for child protection.

The Guidelines should instead reference specific age verification providers that have been assessed and approved by the European Commission as meeting the criteria described.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Pushes for mandatory built-in age and parental controls on all connected devices, and highlights a technically ready 'KidsWallet' system pending broad platform support.

e paper put forward three key proposals: • Mandatory built-in age verification and parental control tools on all devices with Internet access sold in the European market.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Supports interoperable device-level or OS-level age assurance, underscoring shared funding and robust tools for both parents and platforms.

By facilitating interoperable age assurance at the operating system or device account level, we can create a consistent and secure layer of protection that benefits everyone in the ecosystem.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Stresses universal access to age verification, including for non-profits, and welcomes public funding and open source solutions to prevent exclusion.

We welcome government funding for this purpose, as well as a government-funded open source solution.

European Commission Article 28 Guidelines Feedback (unknown). Recommends clearer guidance on when and how to use age assurance, including mechanisms to detect false declarations and proactively identify minors.

While there is good information about age assurance approaches, and platform design, it would be good to add guidelines about when and how to use age assurance in existing platforms and user bases.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Requests explicit definitions and criteria for assessing accessibility to minors, and emphasizes need for measures beyond simply setting age-based terms.

Clarification is necessary on "Not Accessible to Minors". The "Guidelines" clarify that excluding minors based on the terms and conditions of an online platform would not be enough, effective measures are required to avoid minors accessing the service.

DSA (Protection of Minors) Guidelines (Samsung Electronics). Argues for assigning age assurance responsibilities to the platform closest to actual content delivery, favoring in-app over app store-level checks for higher protection.

SE believes the guidelines should reflect that in the case of accessing information through multiple online platforms (e.g., application store download), the online platform in control of and closest to delivering the actual high-risk content (information) to the user should conduct age assurance.

1.3.8 Miscellaneous

This insight addresses the issue of where responsibilities for age verification should be assigned within the digital ecosystem. Specifically, it argues against imposing age verification obligations at the level of app stores, operating systems, or device manufacturers, suggesting that these responsibilities would be misplaced if enforced at these broader infrastructural levels.

Imposer une telle obligation au niveau des magasins d'application, des systèmes d'exploitation ou des terminaux reviendrait à placer la responsabilité au mauvais endroit. (Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM))

1.4 Risk Assessment, Transparency, and Oversight

The most compelling insight across these sub-categories is the shared recognition that effective risk assessment, transparency, and oversight for minors online require clear, evidence-based, and rights-driven frameworks—anchored in independent, multi-layered governance and routine external oversight. Stakeholders consistently argue that "self-regulation and internal assessment alone are insufficient"; instead, platforms should be held to measurable, objective standards, with harmonized definitions and tailored, proportionate obligations that adapt to the specific risks, contexts, and vulnerabilities of minors, including at-risk subgroups. Transparent and ongoing reporting, standardized documentation, and robust third-party audits are seen as essential for meaningful accountability and public trust. The need for collaboration emerges as central: integrating input from children, parents, experts, and civil society at every stage ensures that risk reviews reflect real-world challenges and evolving harms—including those arising from platform design and algorithmic systems. Cross-sectoral alignment and avoidance of regulatory fragmentation—from local adaptation to international interoperability—are repeatedly recommended to reinforce child protection while avoiding unnecessary duplication or loopholes. Crucially, submissions caution against 'techno-determinism' and call for thoughtful, contextual approaches that blend technical solutions with social, legal, and educational interventions. Across all areas, there is a demand for continuous improvement and iterative policy review—ensuring that guidance keeps pace with digital innovation and is openly responsive to emerging risks and best practices. Collectively, these themes highlight the dominance of adaptability, independent oversight, and inclusivity as the cornerstones for safeguarding minors in the digital environment.

1.4.1 Risk Definitions and Scope

The category 'Risk Definitions and Scope' collects diverse but related calls for clearer, more comprehensive, and harmonized definitions of online risks and their scope under the EU Digital Services Act (DSA), especially as they pertain to minors. Insights across documents emphasize the necessity to expand the scope of risk assessments to include a broad range of harms beyond the usual suspects like pornography and gambling, encompassing mental health, discriminatory content, systemic risks, and developmental impacts to children. Stakeholders urge for unambiguous criteria for what constitutes 'high,' 'medium,' or 'low' risk, preferencing objective benchmarks, concrete case studies, and tiered risk taxonomies that ensure consistent and transparent application across platforms and services. There is significant demand for clarification of terms such as 'platforms accessible to minors,' 'significant change,' and expectations around when and how risk assessments must occur. Several submissions highlight the risks of legal uncertainty in areas such as influencer definition, applicability to different gaming and eCommerce platforms, or exemption of SMEs, advocating for clear guidance to ensure no avenue for circumvention or under-protection. Importantly, some recommend adopting or aligning with existing, internationally recognized taxonomies, and broadening risk evaluation to consider both harms and benefits to children's rights and well-being. Underlying these calls is a shared concern that without shared definitions and transparent scoping, platforms may inconsistently interpret obligations, potentially resulting in either inadequate or excessive safeguards. Several insights also stress the need for independent oversight rather than self-evaluation, and for risk recognition to include independent, external evidence about minors' platform usage. Overall, stakeholders urge the Commission to provide more explicit, practical, and rights-centric definitions and expectations to underpin effective risk assessment, mitigation, and oversight.

> *Include the full overview of described harms that VLOPs are having on children, going well beyond what pornography and gambling.* (Ten recommendations to the European Commission to really protect children online (unknown))
>
> *the guidelines do not provide a more specific taxonomy or sufficient examples or case studies to guide providers in consistently classifying specific types of risks as high, medium, or low.* (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))
>
> *Clearer guidance on the criteria for assessing 'accessibility to minors', including a working definition that reflects actual use and service design;* (Protecting children online: response to the draft guidance (DIGITALEUROPE))
>
> *To prevent arbitrary or minimal compliance we recommend defining these risk levels with transparent benchmarks and require independent oversight of risk assessments, rather than relying on platform self-evaluation.* (SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands))
>
> *for example, the DSA does not apply where features with user generated content are low risk and merely ancillary to the overall provision of the general service).* (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))
>
> *In this regard, the guidelines proposed by the Commission would not apply to the small or micro enterprise exempt from DSA, which might be risky as the majority of porn platforms might not be subject to these guidelines.* (Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services))
>
> **Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union).** Advocates for expanding risk assessment scope for Very Large Online Platforms (VLOPs) to comprehensively cover all forms of harm and impacts on children.
>
> **Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild).** Encourages clarification on which platforms, including video games, are covered by the DSA, emphasizing the guidelines' broad scope.

We equally welcome the broad and flexible scope of the guidelines, clarifying Article 28 obligations on platforms which might not be targeting or allowing minors but do not put sufficient measures in place to control it.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Calls for a well-defined risk taxonomy and illustrative examples to guide consistent risk classification and age assurance under the DSA.

the guidelines do not provide a more specific taxonomy or sufficient examples or case studies to guide providers in consistently classifying specific types of risks as high, medium, or low.

WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers). Suggests a legal definition of influencers to mitigate uncertainty and enhance transparency in DSA applicability.

The creation of a legal definition of influencers would be useful to reduce legal uncertainty around the applicability of UCPD to influencers.

CONCLUSION & POLICY DEMANDS (unknown). Stresses that risk assessments must consider both individual and systemic risks affecting minors online.

Online platforms must not only consider risks to individual children but also systemic risks such as normalization of surveillance, commercial pressure, and mental health deterioration.

Ten recommendations to the European Commission to really protect children online (unknown). Urges that risk assessments under the DSA include a full array of harms, covering mental, physical, and developmental risks to minors.

Include the full overview of described harms that VLOPs are having on children, going well beyond what pornography and gambling.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Requests a more explicit definition of the 'best interest of the child' within the context of risk reviews for online minors.

While we welcome the focus on the best interest of the child, in accordance with Articles 3 and 24 of the UNCRC, research shows that the notion of 'best interest' has been misunderstood and misinterpreted by online platforms, at the detriment of children's rights.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Recommends that guidelines focus on clear objectives and outcomes, not just specific solutions, to provide clarity on expected standards.

Finally, the objectives behind certain measures prescribed by the draft guidelines remain unclear.

Additional contribution (Collective Shout). Asks for clarification on whether eCommerce sites are captured under DSA risk typologies.

It is unclear from the Guidelines that eCommerce websites would be sufficiently captured by the 5C risk typology in Annex 1.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Suggests further clarification of the term 'accessible to minors' for determining which platforms fall under DSA Article 28.

According to the draft guidelines, platforms falling in the scope of article 28, are "platforms accessible to minors". Recital 71 and pages 3 and 4 of the guidelines provide clear examples of these platforms. Nevertheless, in our view the guidelines would benefit from further clarification of what is considered as "accessible to minors".

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Proposes referencing DSA Recital 14 and clarifying the scope for Very Large Online Platforms/Search Engines (VLOP/VLOSEs).

AGCOM proposes to include a reference, even in a footnote, to Recital 144 of the DSA, which provides some clarifications on the concept of public disseminatio

DSA_Article_28_GitHub_Response (GitHub). Requests additional guidance on which services are required to conduct risk assessments and what they should entail.

GitHub supports the Guidelines' recommendation for platforms to assess the typology of risks presented to minors based on the 5Cs in Section 5, but recommends that the Commission provide additional clarity regarding which services are expected to conduct such assessments, the scope of these evaluations, and more detailed guidance on what to include in the risk assessment.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Suggests refining the definitions of lootboxes and gambling-like features to aid in proportionate DSA enforcement.

The definition of lootboxes and gambling-like features should be sharpened to provide better guidance for providers and regulators regarding a proportionate exclusion of these elements.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Advocates for clearer, concrete definitions, alignment with international standards, and expanding coverage to online games and rights-based risks.

The Good Practice on p. 34 refers to an "online platform where minors can play games." However, the definition of "online platforms" provided in the DSA excludes many, if not most, online games

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Seeks clear examples of what constitutes 'medium risk' and guidance on when platforms are 'directed to' or 'used by' minors.

It is still necessary to specify what the EU COM actually means by "medium risk."

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Recommends clarifying when feature-level mitigations are required, specifying it should only apply if the core service is an 'online platform.'

it should be clear in Section 6.1.2 that the service must consider feature-level mitigations only if meeting the definition of online platform

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Emphasizes clearly defining risk tiers in age assurance, with transparent benchmarks and independent oversight.

The effectiveness of a tiered risk-based approach depends on clear, objective definitions of what constitutes "high" and "medium" risk.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Highlights the need for legislative findings to acknowledge both risks and benefits of digital services for minors.

California's AADC enumerates ten legislative findings about the Internet's problems, none of which reference the Internet's benefits.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH

LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Suggests adopting a shared risk taxonomy and requiring consistent application across risk assessments using established models.

Leverage an existing risk framework-such as the EU Kids Online model or the OECD four-pillar taxonomy-and require its consistent application across risk assessments, system metrics, and compliance reporting.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recommends defining what qualifies as a 'significant change' to trigger a risk assessment within the guidelines.

A definition of 'significant change' (line 198) should be added to the guidelines.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Requests clarification on whether VLOSEs are covered by Article 28 and, if not, to include them under relevant recommendations.

Les lignes directrices de l'article 28 devraient préciser si elles s'appliquent aux très grands moteurs de recherche en ligne (Very Large Online Search Engines- VLOSEs), car de nombreuses recommandations énoncées par le projet de lignes directrices seraient pertinentes pour ces acteurs.

Microsoft response to the European Commission's draft 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 (Microsoft). Proposes expanding current risk categories to include broader harmful content and suggests that advanced technology is a factor across all risks.

we recommend reconsidering the current framing of risk, as outlined in the table at page 38, which pulls out two specific content risks and excludes other illegal and harmful content risks that may be as impactful, if not more, to young people.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Urges that service providers' awareness of minors on their platforms should include independent third-party evidence, not just internal data.

We are concerned that the interpretation of online services providers' "awareness" under Recital 71 of the Digital Services Act appears too narrowly framed in the guidelines.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Stresses that 'best interest of the child' must be more explicitly defined to prevent misapplication by platforms.

While we welcome the focus on the best interest of the child, in accordance with Articles 3 and 24 of the UNCRC, research shows that the notion of 'best interest' has been misunderstood and misinterpreted by online platforms, at the detriment of children's rights.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Supports a risk-based approach and suggests that social media platforms should be deemed high risk by default.

Welcoming the risk-based approach, but social media platforms should be categorized as high risk per default;

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Advocates for a risk-based approach to platform accessibility to minors instead of a uniform standard.

We believe that the risk-based approach should also be extended to the very concept of a platform's accessibility to minors, as even the simple fact of being accessible does not carry the same risks from platform to platform.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Seeks precision in the definition of 'platforms accessible to minors' and warns about exemptions for small enterprises.

According to the draft guidelines, platforms falling in the scope of article 28, are "platforms accessible to minors".

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Recommends that external scientific evidence be recognized as proof of minors' usage for platform responsibility criteria.

Furthermore, we strongly encourage expanding the definition of the third scenario to include external scientific evidence demonstrating that minors are using the platform or service.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Requests clearer guidance and a working definition of 'accessibility to minors' reflecting actual use and service design.

Clearer guidance on the criteria for assessing 'accessibility to minors', including a working definition that reflects actual use and service design;

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Calls for explanations and evidence behind prescribed solutions in the guidelines, ensuring proportionality and appropriateness.

Where a guideline prescribes a specific issue or solution to provide a high level of privacy, safety and security in the context of recommender systems, the Commission should clearly explain and evidence: (i) the risk(s) or issue(s) that the proposed action/solution is intended to address; and (ii) why the proposed action/solution is a relevant, appropriate and proportionate approach to addressing that risk(s) or issue(s).

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Asks the Commission to clearly define 'significant change' triggering risk review requirements.

Similarly, while we welcome the need to carry out the risk review whenever a significant change takes place, we ask the European Commission to clearly define significant change.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Emphasizes the need for VLOP risk assessments to include a broad scope of harms, especially those affecting mental health and well-being.

Include the full overview of described harms that VLOPs are having on children, going well beyond what pornography and gambling.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Advocates for clearer definitions of risk levels and for impact assessments to weigh positive effects as well as risks.

In the latter case, the impact should be broader than the potential risks posed by online platforms to the rights and well-being of children, and consideration should also be given to the positive impact on their rights and well-being.

DSA (Protection of Minors) Guidelines (Samsung Electronics). Argues for more precise criteria for high-risk content to avoid vagueness and overbroad application.

In the current suggested guideline, the definition of high-risk is quite broad, making it vague to determine the level of risk associated with information, such as content with specific keywords.

1.4.2 Risk Assessment Methodologies and Frameworks

Risk Assessment Methodologies and Frameworks for the protection of minors under the Digital Services Act (DSA) encompass a wide range of recommendations and requirements. Core elements include the necessity for

evidence-based, ongoing, and transparent risk assessments focused on online harms to children and the effectiveness of mitigation strategies. Many stakeholders urge alignment with established frameworks—such as the OECD's 5Cs (Content, Conduct, Contact, Consumer, Cross-cutting), Child Rights Impact Assessments (CRIA), and other international codes—while calling for these assessments to move beyond abstract typologies and reflect real-world risks, including algorithmic and design-related threats. A recurring theme is the importance of integrating risk reviews with existing DSA systemic risk assessment obligations to avoid duplication and overburdening large platforms, while ensuring clarity around thresholds, timelines, and minimum requirements for reviews. The need for assessment processes to be flexible yet rigorous is highlighted, allowing methodological variation but insisting on transparency, documented metrics, and independent or external input (such as audit, expert review, or using academic/civil society data). In addition, multiple documents advocate for targeted risk reviews in contexts such as educational technology platforms and recommend specific tools and minimum standards for operationalizing risk assessment. Collectively, these insights reflect a consensus on the need for risk assessment frameworks to be thorough, data-driven, and child-rights focused, with mechanisms for periodic review and for closing the gap between written policies and actual safety outcomes for minors online.

> *Risk classification must move beyond abstract frameworks. While the OECD's 5Cs typology of risks (Content, Conduct, Contact, Consumer, Cross-cutting) provide a helpful overview, they aren't sufficient as an orientation for providers of online plat- forms to assess their services.* (PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)))
>
> *While CRIAs are mentioned in section 5 (line 200) as a way to support the 5Cs based risk review, they should in fact be the main entry point for the risk review, complemented by the 5Cs framework.* (CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)))
>
> *For VLOPs, annual and "critical" impact risk assessments already exist.* (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))
>
> *Establish a risk-based framework that takes into account, the 5C Typology of risks, the CENELEC framework and how to determine the best interests of the children in the digital environment.* (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))
>
> *New (dimensions of) risks on the platform are consistently identified by sources other than the platform owners, for instance, when new risks are identified via robust empirical research. In such cases, the platform should provide direct communication lines for researchers to send relevant findings to inform risk identification, mitigation strategies and risk reviews.* (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))
>
> *We recommend that the Commission make it more explicit in the Guidelines that any risk review mandated under Article 28 DSA as a result of a significant change to an online platform can be captured by the existing DSA systemic risk assessment process, so as to avoid duplication.* (TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited))

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Advocates for establishing impact baselines and ongoing telemetry before new age verification is introduced, and recommends a 'stacked-risk' model with clear metrics, gradual testing, and phased implementation.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Recommends that educational technology platforms be subject to the same risk assessment and security standards as social platforms, emphasizing this should start at the design stage.

> *Educational technology platforms, widely used in schools - including digital workspaces to connect schools with students and parents widely used upon schools'input - should be subject to the same risk assessment standards and security requirements - right from the design stage - as social platforms.*

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Underscores the need for online platforms to assess and report the effectiveness of their risk mitigation measures for children and includes Child Rights Impact Assessments as a core guideline recommendation.

It is critical that online platforms provide an assessment of the effectiveness of mitigation measures, with relevant data when possible, for ensuring that all the measures adopted are respectful of children's rights and effective in preventing the risks they target, to avoid multiplying ineffective measure that hinders children's experiences online - or do not serve another purpose than protecting children

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Stresses that risk assessments and the need for age assurance mechanisms should be grounded in evidence, not assumptions, and that risks must be re-evaluated continuously as environments evolve.

CIPL would also like to point out that assessment of what constitutes a risk, including a high risk, needs to be based on evidence and may change as research continues to develop.

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Calls for mandatory, algorithmic risk assessments and audits focused specifically on how minors access inappropriate or sexual content.

Mandatory algorithmic risk assessments and audits focused on identifying routes through which minors access sexual content.

Ten recommendations to the European Commission to really protect children online (unknown). Reiterates the requirement that educational technology platforms used in schools should meet stringent risk assessment and security requirements from the outset, similar to social platforms.

Educational technology platforms, widely used in schools - including digital workspaces to connect schools with students and parents widely used upon schools'input - should be subject to the same risk assessment standards and security requirements - right from the design stage - as social platforms.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Encourages improvement of risk assessment and mitigation processes by online platforms as mandated by the DSA, particularly referencing cases where platforms have failed to address demonstrated risks.

TikTok fails to address risks to children and young people's mental health despite past warnings",

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). Recommends that risk assessments for platforms targeted at minors account for the entire content environment, including elements nominally outside the DSA's formal scope.

In terms of risk assessment, where a service is specifically targeted at minors, we consider it important to include the entire content environment of the platform within the risk review.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Highlights new DSA design-focused risk assessment obligations, requiring platforms to assess illegal content risks, ensure algorithmic transparency, and improve UI to curb harm.

EU's Digital Services Act (DSA) includes design-focused regulations that require online platforms to assess and mitigate risks such as illegal content, ensuring transparency in algorithms and improving the design of user interfaces to prevent harmful content from spreading.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Supports DSA-mandated design-focused risk assessments and proposes a tiered risk framework integrating certification, liability, and building codes for safer platform practices.

It proposes a tiered framework that classifies platforms based on design risk and incentivizes safer, more ethical practices through tools like certification, liability, and building codes.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Argues for making Child Rights Impact Assessments mandatory in all systemic risk reviews related to minors.

make Child Rights Impact Assessments (CRIAs) a compulsory component of systemic risk reviews.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Requests more clarity in the DSA guidelines regarding risk review thresholds and decision points, and urges confirmation that existing risk assessments for VLOPs are sufficient for Art. 28 compliance.

Section 4, 5 and 10 of the Draft Guidelines leave providers often absent of clear thresholds or decision points:

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Suggests the guidelines should fill gaps left by the DSA by clarifying how the risk assessment for minors fits with broader systemic risk reviews and by strengthening methodological guidance.

We believe that the guidelines should serve to bolster the risk assessment process and to fill gaps left behind by the DSA, particularly in the absence of specific guidance by the European Commission on how a risk assessment ought to be performed.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Welcomes the integration of Article 28 reviews into broader DSA risk assessments for VLOPs and recommends flexibility in assessment methodology to streamline processes.

We welcome the integration of Article 28 risk reviews into the broader systemic risk assessments for VLOPs (Articles 34 & 35 DSA).

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Calls for risk assessments under the DSA to be extensive, thorough, and include independent expert input to capture risks not readily identified by platforms.

With regard to the risk assessment that the DSA requires platforms to conduct, Bris urges the guidelines to clarify that the assessments must be carried out using an extensive and thorough approach.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Proposes enhancements to risk analysis procedures, specifically recommending inclusion of overexposure and cross-cutting risks associated with minors' online activity.

it is considered useful to include among the types of risk (paragraph 10 - Annex 1 to the Guidelines) also the risk specifically deriving from overexposure related to the intensive use of online platforms by minors, which could be included in the category of so-called "cross- cutting risks," as it identifies a condition that can amplify the negative effects resulting from exposure to illegal or risky content, conducts, and contacts, as well as exacerbate the risks associated with the use of online platforms by minors-consumers.

Policy_demands (unknown). Advocates for educational technology platforms to adhere to the same risk assessment and safety-by-design requirements as social media, due to their similar risk profiles and lack of oversight.

Educational technology platforms, widely used in schools, should be subject to the same standards of risk assessment and safety-by-design requirements as social platforms.

DOT Europe response1 (DOT Europe). Requests clarification of when and how platforms should conduct child rights impact assessments and their relationship to broader risk reviews under the DSA.

We would also encourage the Commission to clarify in what context it is envisaging "child rights impact assessments" (I. 200) to be conducted by online platforms and their relationships with risk reviews.

Consultation on DSA Art. 28 guidelines (The Danish Consumer Council (Forbrugerrådet Tænk)). Emphasizes the importance of using independent, external research sources to accurately determine whether minors are recipients of online services.

When determining when a provider of a platform should be aware that some of the recipients of its service are minors, the guidelines should include substantial, independent and credible evidence from external sources including academic studies, civil society organizations and regulatory bodies.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Critiques reliance on abstract risk typologies and calls for clearer, more actionable risk classification systems for platforms to better assess risks.

Risk classification must move beyond abstract frameworks. While the OECD's 5Cs typology of risks (Content, Conduct, Contact, Consumer, Cross-cutting) provide a helpful overview, they aren't sufficient as an orientation for providers of online plat- forms to assess their services.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Agrees with using the 5C typology to orient risk reviews but notes a lack of concrete guidance on the regular steps platforms should take when risks are identified.

Orientation towards the 5C typology is useful in the context of the risk review.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Supports the use of established CRIA frameworks (UNICEF, Dutch Code, 5Rights) for risk reviews and argues reviews should respond to new/increased risks, not just major platform changes.

We support the promotion of CRIAs and suggest referring explicitly to established frameworks by UNICEF, the Dutch Code for Children's Rights, or the 5Rights Foundation.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Advocates for Child Rights Impact Assessments prior to launching features accessible to minors, with independent certified assessor oversight.

Scope: Before launching features accessible to minors

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Recommends allowing diverse but transparent and appropriate risk assessment methodologies beyond the traditional 5C typology, and affirms that no extra assessments are needed beyond existing reviews for significant changes.

Acknowledging existing efforts, the guidelines should also allow for diverging methodologies and metrics (beyond the 5C typology) provided they are transparent and appropriate to identify risks.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Argues that risk assessments should precede the requirement for age verification on 18+ services and calls for clearer differentiation between risk types in product versus content recommender systems.

we are arguing against the guidelines' approach of assuming that an 18+ age restriction automatically means that there are "identified risks to minors", meaning that the website must institute age verification.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Reinforces the need for CRIAs for all new features accessible to minors, supported by independent review.

Scope: Before launching features accessible to minors

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Endorses the OECD's 5C framework and recommends providing practical tools and templates to support operationalization of risk assessments for diverse online platforms.

We welcome the Commission's endorsement of the OECD's 5C typology of risks - a valuable conceptual tool to classify the types of harms minors may encounter online (Content, Contact, Conduct, Consumer and Cross-cutting risks). This framework provides a strong foundation to structure risk assessments across platforms of different sizes and sectors.

Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus). Proposes a structured risk management matrix that closely links identified risks, mitigation measures, and ongoing monitoring; advocates CRIAs across all aspects of design and operation.

We propose enhancing this requirement by introducing a structured risk management matrix, clearly linking:

STATEMENT (Digipeace (Digirauha ry)). Highlights ambiguities in the DSA risk assessment guidelines and calls for specified minimum requirements, schedules, and transparency, with expedited reviews for urgent threats.

There is still quite a lot of ambiguity in the Guidelines which may create delays and inconsistent compliance.

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Supports risk management obligations for platforms, particularly those with vulnerable users, to minimize risks through regulated processes.

The European Commission assesses that the scope of the guidelines is to minimize risks arising from platform activities.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Suggests that effectiveness metrics and robust evaluation frameworks are essential for DSA compliance; recommends that platforms also assess algorithmic risks using standards such as the 5C Typology and CENELEC.

How will the European Commission measure the tangible difference these interventions make in children's digital experiences? What indicators will demonstrate progress compared to pre-regulation baselines? Establishing robust evaluation frameworks with clear metrics will be essential to assess whether regulatory objectives translate into meaningful protection improvements for young users.

Feedback DSA (unknown). Argues that risk assessment should shift from being the sole responsibility of platforms to independent authorities guided by scientific expertise.

Platforms are currently expected to assess content risk, but this places a heavy burden on industry actors who may lack the expertise or incentive to do so objectively.

Feedback on EC draft guidelines for the protection of minors online under the DSA (unknown). Advocates for including recurring, representative survey data in platform risk assessments to better measure and address harms to minors.

The EC should include guidance that, for conduct- and contact-based harms, platform risk assessments include data from representative surveys that measure population prevalence, severity, and remediation.

Microsoft response to the European Commission's draft 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 (Microsoft). Recommends clarifying the threshold for risk reviews with a focus on the highest risks to minors and emphasizes rights-based product development and risk mitigation.

We recommend clarifying the threshold for risk review and a focus on mitigating the highest risks to minors.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Promotes harmonization of DSA risk assessment with the EU AI Act's risk classification frameworks for consistent protection regarding AI-driven systems involving minors.

Promote alignment with the EU Al Act's risk classification frameworks to identify high-risk systems involving minors, ensuring coherence with broader legislative safeguards.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Stresses that new features for minors should require a pre-launch Child Rights Impact Assessment conducted by independent certified assessors.

Scope: Before launching features accessible to minors

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Recommends reporting structures and risk analysis for detecting and addressing addictive or compulsive use behaviors among minors, including risks stemming from design.

Ergänzungsvorschlag BMASGPK: Einführung einer Meldekategorie für suchtartiges oder zwanghaftes Nutzungsverhalten.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Suggests that CRIAs, rather than just the 5Cs typology, should be the primary basis for risk reviews, with the 5Cs serving as a complement.

While CRIAs are mentioned in section 5 (line 200) as a way to support the 5Cs based risk review, they should in fact be the main entry point for the risk review, complemented by the 5Cs framework.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Urges that risk assessment requirements for VLOPs be streamlined to avoid duplication by recognizing the sufficiency of existing assessments, and calls for flexible, transparent methodologies.

In the interest of further streamlining risk assessment requirements for providers of VLOPs, we invite the Commission to clarify that carrying out a critical impact risk assessment for the purposes of Article 34(1) is sufficient to discharge such providers' duty to carry out a risk review upon making a significant change for the purposes of Article 28(1) DSA and the Guidelines.

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 (European Commission). Outlines DSA provisions requiring risk assessment and mitigation, especially regarding recommender systems and functional settings affecting minors' privacy and safety.

This includes the following provisions of Regulation (EU) 2022/2065: Articles 34 and 35 on Risk assessment and Mitigation of risks, Article 38 on Recommender systems, Article 40 on Data access and scrutiny and Article 44 (j) on standards for targeted measures to protect minors online.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des

Droits de l'Homme (CNCDH)). Underscores the need for prompt adoption of guidelines detailing risk assessment methodologies and tools to gauge measure effectiveness for platforms accessible to minors.

il paraît essentiel que la Commission adopte dans les plus brefs délais des orientations à destination des plateformes afin de préciser la méthodologie d'évaluation des risques et les outils pour mesurer l'efficacité des mesures adoptées par chaque plateforme pour limiter ces risques.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Emphasizes mandatory review cycles, risk reviews, age-based restrictions, safeguards for AI tools targeting minors, and the role of external audits and technical safeguards for complex services ('super-apps').

Instead, it advocates for clearly defined review cycles, with mandatory consultations triggered by significant platform changes.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Stresses proactive, ongoing risk mitigation for minors, including use of measurement, empirical research, and embedding minor-focused risk review in systemic assessments under the DSA.

While this paper is largely focused on the United States context, many of the recommendations related to measurement are directly relevant for proactive and ongoing mitigation of risks to minors.

Contribution from medical professionals regarding the Draft Commission Guidelines on the Protection of Minors Online (Article 28 DSA) (Youth Smoking Prevention Foundation (Stichting Rookpreventie Jeugd); #vapenjouwkeuze). Highlights the importance of ensuring platforms' risk assessments are accurate and context-sensitive, especially regarding real-world exposures such as illegal vape marketing.

A fundamental issue that the Guidelines must address is the serious and widespread exposure of minors to illegal and harmful content – particularly the marketing and sale of illegal vapes – through online platforms.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Requests explicit clarification that platform risk reviews after significant changes can be addressed within existing systemic risk assessments under the DSA.

We recommend that the Commission make it more explicit in the Guidelines that any risk review mandated under Article 28 DSA as a result of a significant change to an online platform can be captured by the existing DSA systemic risk assessment process, so as to avoid duplication.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Encourages regular, child-specific risk assessments that go beyond age verification to encompass systemic risks such as addictive engagement, monetization schemes, and exposure to harmful content.

Child-specific risk assessments need to be conducted on a regular basis across the life cycle of digital services directed at children and should go beyond age verification and assess systematic risks such as those related to addictive engagement loops, coercive monetization strategies, and exposure to harmful or age-inappropriate content.

Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation). Supports mandatory, audited, and inclusive CRIAs for platforms and assessment of both positive and negative effects of risk measures on children's rights.

We also support the requirement for platforms to assess in their risk review the potential positive and negative effects on children's rights of any measure they may or will have in place.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Recommends incorporating the precautionary principle in child safety risk approaches and calls for clear impact assessment methodologies for platforms.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Asserts that existing risk assessments should be accepted as fulfilling the guidelines' expectations to avoid unnecessary duplication.

Recognition that existing risk assessments should be considered sufficient to meet the "Guidelines" expectations, avoiding unnecessary duplication.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). Criticizes the lack of clarity and specificity in draft risk assessment procedures and categories, leading to potential overclassification and uncertainty.

The draft is not concise in regards to how a risk assessment should be done.

DSA (Protection of Minors) Guidelines (Samsung Electronics). Advocates for an EU-led, unified guide for application risk assessment to provide consistency and efficiency across platforms.

SE believes that an EU-led guide for assessing the risk of applications is essential.

Position du groupe La Poste (La Poste). Suggests that platforms be permitted to self-assess the risks of their recommendation systems and implement proportionate mitigations tailored to user context.

Nous recommandons que les plateformes en ligne soient autorisées à évaluer elles- mêmes les risques spécifiques associés à leurs propres systèmes de recommandation, en fonction de leur nature et de leur finalité.

1.4.3 Proportionality, Flexibility, and Differentiation

The insights across these documents emphasize the critical importance of proportionality, flexibility, and differentiation in the risk assessment, transparency, and oversight of online platforms with regard to the protection of minors under the Digital Services Act (DSA). There is broad consensus that regulatory measures should be tailored to the varying degrees of risk posed by different services, platform types, and audience profiles. One-size-fits-all mandates are discouraged, as they could lead to overregulation, unintended consequences, or disproportionate burdens, particularly on lower-risk or niche platforms. Stakeholders advocate for a risk-based approach, wherein mitigation strategies and compliance obligations are scaled according to the nature, functionality, and specific risk profiles of each platform. The guidelines should allow for adaptation to rapid technological change, local context, platform diversity, and differing needs across age groups or user types. Additionally, several contributors point to the significance of thorough impact assessments that weigh both potential benefits and drawbacks—not only for minors, but for all users and fundamental rights—with transparency around the rationale for chosen measures. The documents also highlight the necessity to acknowledge technical feasibility, sectoral expertise, existing safeguards, and the dynamic nature of digital innovation. Overall, an effective and rights-respecting regulatory framework is characterized by clear but adaptable guidance, capacity for platforms to justify alternative, equally effective measures, and explicit mechanisms for proportionality and differentiation. Such a framework seeks to protect minors without stifling innovation, infringing on users' rights, or imposing undue burdens where risks are low.

We believe this recommendation could be achieved simply, by establishing Proportionality as the primary, overarching general principle. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

A targeted, risk-based framework will more effectively protect minors while maintaining the dynamism and competitiveness of the European digital ecosystem. (Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance))

The risk-based approach proposed in the guidelines (lines 147-158) is appropriate given the breadth of online platforms in scope of the DSA. (Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games))

There is a tangible risk that automated moderation or advertising restriction tools, if not nuanced, may inadvertently classify low-risk lottery content alongside high-risk gambling, leading to undue restrictions. (The European Lotteries' Response to Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act (The European Lotteries))

These measures may be appropriate for high-risk platforms or services specifically targeting minors, but applying them indiscriminately risks undermining user experience, distorting business models, and introducing unnecessary friction on low-risk platforms. (Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance))

Platforms prioritize dominant languages, ignoring diverse communities due to limited profitability. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). This document stresses that risk reviews for the protection of minors should account for adverse effects on all users, advocating for thorough and balanced assessments to avoid disproportionate harm to broader user rights.

BDZV MVFP Reply to EC Art 28 DSA Draft Guidelines (BDZV Bundesverband Digitalpublisher und Zeitungsverleger e. V.; MVFP Medienverband der freien Presse e. V.). Editorial online platforms argue for exclusion from additional DSA safeguards, emphasizing that proportionality and platform-specific characteristics must guide regulatory obligations, especially regarding minors' access.

The specific features of editorial online platforms of press publications shield minors from online harms in an appropriate and proportionate manner.

Stellungnahmen zum Leitlinienentwurf zum Minderjährigenschutz im Digital Services Act (Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)). It is highlighted that guidelines should exempt low-risk, user-generated content and account for differences in online platform business models, particularly for minor protection.

Deshalb sollte im Abschnitt 6.1.2 klargestellt werden, dass die Verpflichtungen keine Anwendung finden, wenn es sich um user- generierten Inhalt mit geringem Risiko handelt oder dieser nur eine Nebenfunktion bei der Erbringung des allgemeinen Dienstes darstellt.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). The document advocates evaluating both positive and negative impacts of protective measures on children's rights to ensure proportionality and avoid undue restriction of their freedoms.

The potential positive and negative effects on children's rights of any measure that the provider currently has in place and any additional measures, ensuring that these rights are not disproportionately or unduly restricted.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). This submission recommends that certain inherently low-risk services, like financial and healthcare platforms, could be exempt from detailed risk assessment obligations due to their nature.

CIPL would also recommend considering whether certain services can be excluded from the obligation to do such an assessment due to their nature (e.g., financial institutions, healthcare, food and hospitality, and travel).

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). Tailoring risk guidance and safeguards for minors according to different age groups and needs is recommended, rather than relying solely on platform-wide risk metrics.

we believe that the guidelines could more fully reflect the differing needs of minors across various age groups and provide tailored guidance and safeguards accordingly.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). The document calls for regulatory frameworks to avoid Eurocentric

or one-size-fits-all approaches and to be sensitive to diverse local and cultural contexts in digital regulation.

Technology platforms from Western countries often prioritize Western norms and values, which can marginalize local contexts and create products unsuited for the Global South.

Comments on the European Commission draft 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 ("DSA") (BDZV, MVFP). It urges that editorial platforms be excluded from Article 28(4) guidelines, stating that further measures would be disproportionate and unnecessary given their low risk to minors.

We call on the Commission to exclude all editorial online platforms from the scope of the forthcoming Article 28(4) guidelines.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). This response argues for increased flexibility and proportionality in the Guidelines, noting that overly prescriptive, one-size-fits-all measures do not account for provider differences or technical feasibility.

We note that while the Draft Guidelines set out that it depends on the risk review what to implement, the measures which are proposed are at times rather prescriptive / geared towards a one-size-fits-all approach.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). AFNUM supports a coherent, proportionate, risk-based approach that leaves room for innovation and recognizes established arrangements under the Digital Services Act.

Nous estimons qu'une approche proportionnée, fondée sur les risques, laissant une marge d'innovation aux acteurs et valorisant les dispositifs existants, constitue la voie la plus efficace pour protéger les mineurs en ligne tout en préservant un environnement numérique dynamique, sûr, inclusif et respectueux des droits fondamentaux.

ACT RESPONSE TO THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Association of Commercial Television and Video on Demand in Europe (ACT)). The ACT cautions against blanket, mandatory age verification across platforms, underscoring that proportionate, context-sensitive approaches avoid harming user experience.

These measures might suit their platform but would likely unnecessarily impair the consumer experience on our services.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). CDT Europe requests clarification of the risk review framework for more consistent and proportionate applications, flagging risks of unequal fundamental rights protection across the EU.

This fragmentation may be further aggravated by the fact that the conceptual framework of the Risk review is itself in need of further clarity, but also the fact that DSA oversight and enforcement at national level is taking place at various speeds and levels of effectiveness. This risks impacting the fundamental rights of Europeans across the Union unequally.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). AMETIC recommends allowing feature-specific risk assessment and mitigation, instead of blanket feature bans, to foster proportionate obligations and higher quality user experiences.

Furthermore, platforms should be allowed to conduct feature-specific risk assessments and apply targeted mitigations.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA

Europe)). CCIA Europe emphasizes the need for flexibility in the Guidelines to allow platforms to adjust to emerging risks and avoid imposing uniform requirements on non-high-risk platforms.

Given the fast-changing environment, it is essential that the measures recommended by the Commission still allow online services to quickly adapt to emerging trends and risks.

Amazon's contribution to the Guidelines on the protection of minors under Article 28 of the Digital Services Act (DSA) (Amazon). Amazon underlines that protective measures should depend on the specific risk of harm to minors and the nature of the platform, advocating against one-size-fits-all implementations.

For all services in scope of DSA Article 28, selecting where to include protection measures (e.g., age assurance / verification) will not be a one-size-fits-all solution and will be highly dependent on where the risk of harm to minors lies on the service, as well as the technical scalability of incorporating such measures at different levels.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Video Games Europe urges that the right to play be factored into the proportionality assessment for any measure affecting children's platform access.

VIDEO GAMES EUROPE therefore recommends that the Guidelines should acknowledge more clearly the right to play, and its importance for the proportionality test.

DOT Europe response1 (DOT Europe). DOT Europe supports flexibility and proportionality, suggesting that Guidelines allow for risk- and service-specific implementation without rigid design mandates.

As such, they should be flexible as regards different design features.

Consultation on DSA Art. 28 guidelines (The Danish Consumer Council (Forbrugerrådet Tænk)). The Danish Consumer Council emphasizes transparency, recommending that providers explain their proportionality assessments and conduct case-by-case reviews for each risk measure.

Platform providers should explain how they estimate the proportionality and appropriateness of the measures identified in their risk review.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Snap champions proportionality as the overarching principle, proposing a final balancing test to ensure context-sensitive, risk-based recommendations in the Guidelines.

We believe this recommendation could be achieved simply, by establishing Proportionality as the primary, overarching general principle.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). The Integrity Institute recommends that risk assessment frameworks be scalable so resource demands reflect platform size and risk level, ensuring proportionality.

It is our recommendation that scalable risk assessment frameworks are considered to ensure that the resource constraints are proportionate across smaller services and VLOPs.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). This response stresses the need for detailed presentation of balancing aspects and proportionality judgments in risk reviews to ensure providers' perspectives are adequately considered.

The assessment of proportionality is a value judgment that can vary significantly depending on the individual case.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Adigital calls for a balance between prescriptiveness and flexibility in the Guidelines to effectively address potential harms to minors.

To effectively mitigate risks, it is essential to strike a balance between providing clear guidance and allowing for flexibility in implementation.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). The Working Group on Gaming and Regulation supports a risk-based approach that preserves proportionality and considers the broader rights and impacts on all users, not just minors.

We also support the risk-based approach outlined in Section 5, which helps ensure that measures are proportionate and protect the rights of all users.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Ecommerce Europe suggests introducing a 'low-risk platforms' category and shaping obligations proportionally to better reflect service diversity and varying minor-related risks.

the current binary classification of platforms into either "high-risk" or "moderate-risk" categories fails to capture the real different levels of risks for minors, the diversity of services and of user profiles.

The European Lotteries' Response to Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act (The European Lotteries). The European Lotteries advocate for a risk-differentiated, proportionate DSA implementation that respects national frameworks and safeguards low-risk lottery service integrity.

A successful implementation must be rooted in risk differentiation, proportionality and respect for national regulatory frameworks.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). This analysis argues that regulatory interventions must consciously weigh trade-offs, recognizing that not all children benefit equally and avoiding rigid one-size-fits-all approaches.

As a result, regulatory restrictions on Instagram access would likely benefit some minors, but at the cost of increasing the psychological or mental distress of other minors.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). The Working Group echoes support for proportional, risk-based guidelines that also account for effects on all users, not only children.

We also support the risk-based approach outlined in Section 5, which helps ensure that measures are proportionate and protect the rights of all users.

Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance). The European Tech Alliance calls for the risk framework to reflect real platform differences, including a third, low-risk tier, and for default settings to be proportionate to assessed risk.

A targeted, risk-based framework will more effectively protect minors while maintaining the dynamism and competitiveness of the European digital ecosystem.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis highlights the challenge of aligning well-intentioned policy with technical feasibility and calls for clearer criteria for determining appropriate and proportionate measures.

Finally, Homo Digitalis, believes that despite well-intentioned policy goals, fundamental incompatibilities with current technical capabilities may be presented, and recommend that future regulatory initiatives incorporate greater consideration of technical feasibility to ensure that policy

objectives can be meaningfully achieved within existing technological paradigms, rather than mandating solutions that exceed current technical possibilities.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). The Advertising Information Group urges more proportional, flexible guidelines considering varied platform audiences and features, and suggests that editorial platforms be exempt where existing protection suffices.

However, given that platforms can differ in terms of their audiences and features, we advocate for increased proportionality and flexibility in the final version of the guidelines.

FEEDBACK: European Commission draft 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 (European Magazine Media Association (EMMA) and European Newspaper Publishers' Association (ENPA)). EMMA and ENPA stress that the guidelines' definitions and requirements must be proportionate and differentiate between social media and low-risk editorial platforms.

The clarifications provided in the guidelines regarding what constitutes an online platform "accessible to minors" must be proportionate and not overly broad.

Microsoft response to the European Commission's draft 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 (Microsoft). Microsoft welcomes a proportional, flexible approach in the Guidelines recognizing child rights and variation in platform governance structures.

We welcome the emphasis on proportionality and the flexible approach put forward.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Google welcomes that the Guidelines acknowledge platform differences and considers that their level of detail may surpass typical best-practice guidance, risking inflexibility.

The Guidelines are exceptionally detailed, outlining a vast array of measures to ensure a high level of privacy, safety and security for minors. We therefore welcome the recognition from the Commission that "different online platforms may pose different types of risks for minors" and that "it will not always be proportionate for all providers of online platforms to apply all the measures described in these guidelines".

Position of Polish Confederation Lewiatan on Commission's consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan). The Polish Confederation Lewiatan calls for flexibility so platforms can implement risk- and function-specific solutions, warning against blanket rules.

To effectively mitigate risks, it is essential to strike a balance between providing clear guidance and allowing for flexibility in implementation.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Middle Tech Europe recommends that DSA measures be targeted to actual risk for minors, and opposes disproportionately burdensome requirements on mid-sized platforms.

On a related note, some of the recommendations not only go much further than the obligations set out in the DSA (care should be taken not to impose measures exceeding the DSA's scope, at risk of legal overreach), but they also seem like they would be disproportionately burdensome for midsized platforms.

Ten recommendations to the European Commission to really protect children online (unknown). This document advocates for extending DSA risk and safety requirements to educational tech platforms used by children, rather than only major social platforms.

Educational technology platforms, widely used in schools, should be subject to the same standards of risk assessment and safety-by-design requirements as social platforms.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Vodafone welcomes the emphasis on adaptability, proportionality, and flexibility in the Guidelines to accommodate evolving digital services.

Proportionality and Flexibility: We welcome the emphasis on proportionality and encourage the Commission to ensure that the guidelines remain adaptable to the diverse nature of digital services and evolving technologies.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Epic Games supports the DSA's risk-based, proportionate approach, balancing protection with children's rights to participation and self-expression online.

The risk-based approach proposed in the guidelines (lines 147-158) is appropriate given the breadth of online platforms in scope of the DSA.

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). LinkedIn urges the Commission to sustain risk-based, proportionate Guidelines allowing bespoke measures tailored to individual platform risk profiles.

In keeping with the purpose and spirit of the Digital Services Act (DSA), we urge the Commission to maintain a risk-based and proportionate approach within the Guidelines.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Snap calls for proportional, risk-based, flexible recommendations, warning that rigid measures not matched to platforms' real risks can cause harm.

Measures that are too rigid, overly broad, or divorced from technical and developmental realities risk not only ineffectiveness but unintended harm.

Protecting children online: response to the draft guidance (DIGITALEUROPE). DIGITALEUROPE strongly supports flexible, risk-based, and proportionate measures in the Guidelines, stressing that protection should remain enabling rather than exclusionary.

We strongly support the draft's emphasis on risk-based, flexible measures, and its recognition that protection does not mean exclusion.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). TikTok cautions against prescriptive guidelines, advocating for risk-based, proportionate approaches in line with the DSA's intention of contextual appropriateness.

Article 28(1) DSA requires measures put in place to ensure a high level of privacy, safety and security to be appropriate. In contrast, however, in places, the Guidelines are highly prescriptive. Such an approach prevents providers from assessing whether the recommended measures are indeed appropriate for their platform or the risks that they pose.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Leiden Law School urges the Guidelines to underscore proportionality to ensure full respect for the spectrum of children's rights, including participation and protection.

In this context, greater emphasis should be placed on the proportionality of measures regarding measures that respect all children's rights, i.e. children's participation, protection and provision rights.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). PEGI requests that the Guidelines allow risk assessment and proportionality to determine if parental controls are sufficient for compliance, opposing blanket mandates.

PEGI requests that the Guidelines should make it clear that the risk assessment and consideration of the general principles, such as proportionality, should be used to determine if parental controls alone can satisfy the requirements of Article 28(1) DS

DSA (Protection of Minors) Guidelines (Samsung Electronics). Samsung Electronics argues that the app store's role in risk assessment is limited as they rely on developer-supplied information, so proportionality is needed when assigning responsibilities.

Furthermore, the responsibility of app store providers in the risk assessment process is limited.

Position du groupe La Poste (La Poste). La Poste asserts that DSA rules should be customized according to service providers' diversity and not uniformly applied, recognizing distinct business models and responsibilities.

il est essentiel de veiller à ce que ces règles ne soient pas appliquées de manière uniforme à l'ensemble des acteurs et des services numériques.

1.4.4 Standardization, Certification, and Benchmarks

This category emphasizes the urgent need to establish concrete, consistent, and measurable standards and benchmarks for risk assessment, transparency, and oversight in digital services—especially regarding minors' privacy, safety, and security. Multiple stakeholders highlight the challenges of vague definitions (such as "accuracy," "trustworthy," or "harmful") and warn that without standardization, risk evaluations and mitigation efforts will vary significantly between providers, leading to inconsistencies and reduced effectiveness. Contributions call for the development of common risk matrices, standardized reporting formats, data standards, tiered certification schemes, and objective benchmarks that would allow for meaningful comparison, accountability, and external oversight. The importance of leveraging existing co-regulatory frameworks and harmonizing new requirements with established systems is repeatedly stressed. Additionally, some insights advocate for technical measures (like digital watermarking), clearer documentation (such as technical annexes and non-compliant feature lists), and greater transparency enabled by public reporting and third-party audits. Overall, a unifying theme is the recognition that only through clear, objective, and enforceable standards—backed by robust certification and transparent metrics—can digital platforms be held reliably accountable for risks to children and the wider digital public.

We call on the Commission to benchmark each category of risk to minors' privacy, safety or security. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

More clarity is needed in terms of oversight and certification to avoid inconsistent standards. (Yoti_response_on_Article_28__2_.pdf (Yoti))

Issue a living Technical Annex: Develop a dynamic technical annex that defines minimum safety baselines, standardised metrics (e.g. exposure-diversity index, true/false positive rates by protected attribute), and exemplar testing protocols. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Risk disclosures should follow a standardised reporting format and mandated reporting timeline and include essential indicators. (CONCLUSION & POLICY DEMANDS (unknown))

Standardize and develop norms and mechanisms for Flaw and Design Disclosure to ensure developers receive timely, constructive feedback while protecting researchers. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

In today's digital world, metrics are the invisible currency that guides design choices, business models, and social norms. They function as price signals-proxies for value that determine where attention, investment, and innovation flow. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Calls for benchmarking risk categories to minors' privacy, safety, and security, cautioning that lack of clear definitions will result in inconsistent identification of risks across platforms.

CONCLUSION & POLICY DEMANDS (unknown). Recommends standardized formats and mandatory timelines for risk reporting under the DSA, aiming to facilitate independent analysis and public monitoring.

This enables independent analysis and comparison across platforms.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Advocates for a tiered system of prosocial tech standards, certification, data standards, and standardized disclosure mechanisms to integrate ethical principles into platform design.

Just as cities enforce building codes for housing to ensure public safety and urban planning, investors, regulators, and companies could also develop tech platform building codes to reduce harm and contribute to public goods.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Emphasizes adopting data standards, evidence-based metrics, and tiered certification to guide and evaluate ethical platform design and trustworthiness.

In today's digital world, metrics are the invisible currency that guides design choices, business models, and social norms. They function as price signals-proxies for value that determine where attention, investment, and innovation flow.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Highlights the need for more granular and consistent guidelines, along with clear criteria and resources for trusted entities in risk identification and dispute settlement.

It is worth noting that the Guidelines status as guidance and the use of flexible language creates interpretive space that may complicate consistent implementation and undermine fair competition between platforms who possess or are able to deploy the resources to meet the expectations of 'European Board for Digital Services' (the 'Board') and those who don't.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Urges that established co-regulatory frameworks like PEGI and USK be respected, warning that new DSA guidelines should not create fragmentation or undermine these systems.

By introducing fragmentation within the sector, the Guidelines risk undermining established co-regulatory frameworks like PEGI and the USK system.

Yoti_response_on_Article_28__2_.pdf (Yoti). Calls for more clarity and transparency in oversight and certification to prevent inconsistent standards, supporting certification schemes and conformity assessments.

More clarity is needed in terms of oversight and certification to avoid inconsistent standards.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Proposes using established assessment criteria to build uniform standards, ensuring effective and consistent provider oversight and risk review.

This assessment criteria could be used to create uniform standards to guarantee orientation regarding an effective risk review.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Supports establishing transparency and benchmarking of minimum standards, noting the need for more attention to concrete and detailed exemplary measures.

The guidelines include many concrete examples of potential measures or features to be adopted by companies.

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). Stresses the importance of clear definitions and measurable performance thresholds, noting that vague terms hinder the design and testing of compliant systems.

Terms such as "accuracy", "trusted ID" and "reliable estimation" are vague.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Recommends using objective, unambiguous terminology for concepts like age-appropriateness and harm to ensure consistent implementation across platforms.

The guidelines should adopt more objective and unambiguous terminology.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Advocates for adding more detailed specifications and benchmarks to the proposed measures to improve the effectiveness of the guidelines.

To further strengthen the guidelines, we recommend adding further detail on the measures proposed, including specifications and benchmarks in a number of areas.

STATEMENT (Digipeace (Digirauha ry)). Repeats the call to reinforce guidelines with greater detail on measures, specifications, and benchmarks, aligning with 5RightsFoundation recommendations.

We join the 5RightsFoundations in their recommendations to further strengthen the guidelines by adding further detail on the measures proposed, including specifications and benchmarks in a number of areas.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Suggests issuing a dynamic technical annex with minimum safety baselines, standardized metrics, and protocols, and recommends third-party auditing and provider transparency regarding adopted metrics.

Issue a living Technical Annex: Develop a dynamic technical annex that defines minimum safety baselines, standardised metrics (e.g. exposure-diversity index, true/false positive rates by protected attribute), and exemplar testing protocols.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Encourages enhancing the guidelines with further detail, specifications, and performance benchmarks in critical areas to ensure robust protection for minors.

To further strengthen the guidelines, we recommend adding further detail on the measures proposed, including specifications and benchmarks in a number of areas.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Proposes investment in technical solutions like digital watermarking and cryptographic signatures for verifying content authenticity and provenance to support compliance and risk management.

Investing in and implementing advanced technical solutions for content provenance and authenticity, such as digital watermarking and cryptographic signatures, that can be embedded at the point of AI generation.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Suggests the publication of a non-exhaustive list of non-compliant platform functions to aid in standardizing online interface design expectations.

We suggest that the Commission makes a non-extensive list of functions or features that would not be compliant with Article 28 in the DSA, and the guidelines in regard of online interface design and other tools.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Emphasizes the use of measurable and testable standards (like IEEE 7001-2021) to assess and certify transparency in autonomous systems.

IEEE 7001-2021TM Standard for Transparency of Autonomous Systems establishes measurable, testable levels of transparency, so that autonomous systems can be objectively assessed, and levels of compliance determined.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Recommends adding detailed benchmarks and clear definitions for risk levels (e.g., in age assurance), subjecting assessments to external oversight instead of company self-assessment.

a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks. Additionally, the assessment should be subject to external oversight, avoiding self-assessment by companies. The potential for age assurance to also complement age appropriate design should be clearly recognised.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Stresses the need for effective metrics to evaluate the success of preventive or mitigating measures for protecting children online under the DSA.

1.4.5 Transparency, Disclosure, and Reporting

The collected insights emphasize a strong consensus on the need for enhanced transparency, disclosure, and reporting by online platforms regarding their risk assessments, especially as they pertain to minors under the Digital Services Act (DSA). A significant number of stakeholders call for mandatory, timely, and standardized public publication of both the outcomes and methodologies of risk reviews, arguing that weak or non-binding language ('consider publishing') is insufficient and leaves room for platforms to conceal or underreport risks. Many advocate for risk assessment results to be accessible not just to regulators, but also to researchers, civil society, and the public, with some recommending versions tailored for children or non-expert audiences to empower informed decision-making. There is also a clear interest in ongoing, periodic transparency reporting that details concrete mitigation measures taken, potential algorithmic impacts, moderation practices, and the effectiveness of features like age estimation and content controls. Several contributors stress the importance of independent audits and impact assessments, as well as accessible, machine-readable formats to facilitate oversight and evidence-based policy evaluation. However, some caution against full public disclosure, raising concerns about sensitive information and trade secrets, and propose limited disclosure to authorities or vetted researchers instead. Finally, stakeholders acknowledge the limits of transparency alone and underscore the need for robust oversight and alignment with broader accountability mechanisms.

Moreover, platforms should be required to publish not only the outcomes but also the methodology and process used in conducting the risk assessment. (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 Feedback (Gesellschaft für Freiheitsrechte e.V.))

Demand timely publication of risk review assessments in accessible machine readable formats. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Demand timely publication of risk review assessments in accessible machine readable formats. (CONCLUSION & POLICY DEMANDS (unknown))

we recommend introducing a requirement that platforms publish the results of their risk assessments for oversight purposes. (Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus))

We note that these risk reviews may contain sensitive information, which bad actors could exploit to undermine measures put in place by providers to protect minors on their online platforms. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

The results of this research need to be available to independent researchers (this should feed into Article 40); and to other stakeholders (i.e. such research cannot be kept unpublished if the results are

not favourable to platforms) (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Argues for stronger transparency obligations requiring online platforms to publish not just outcomes but also detailed methodologies for their risk reviews, removing vague language to ensure accountability.

Moreover, platforms should be required to publish not only the outcomes but also the methodology and process used in conducting the risk assessment.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Urges mandatory, timely publication of risk assessment outcomes in accessible, machine-readable formats, warning that lack of requirements allows platforms to conceal risks.

The guidelines currently do not include any requirements for platforms to publish their risk assessments and hence leave it up to Online Platforms to decide and potentially conceal risks.

Contribution Guidelines art 28 DSA (Respect Zone). Advocates for enhanced algorithmic transparency and the enhancement of user control, emphasizing clear disclosures on how platforms operate.

Urgent Concerns Regarding Online Marketing to Children on Digital Streaming Platforms and the Adequacy of Current Regulations (Inria). Highlights the lack of transparency in ad targeting on children's content, calling for meaningful explanations for minors about why they see certain ads.

Unlike ads shown on other content, where users can typically access a "Why am I seeing this ad?" feature explaining the personalization factors, this transparency is unavailable for children's content.

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Commits to transparent reporting to regulatory authorities, including segmented statistics and dashboards to track and report user behaviors and compliance measures.

From day one of Phase 1, we will provide selected and relevant statistics to the Commission, the European Board for Digital Services, and the Cyprus Radio Television Authority (CRTA) as DSC for Aylo's EU main establishment in Cyprus.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Recommends standardized, timely, and publicly accessible disclosure of risk assessment reports by platforms to facilitate monitoring and evidence-based policy.

Demand timely publication of risk review assessments in accessible machine readable formats.

Response to the European Commission's Consultation on the Draft Guidelines for Article 28 of the Digital Services Act (DSA) (European Commission). Calls for full transparency from the European Commission regarding the purposes and expected outcomes of initiatives like the mini-ID wallet in terms of data protection.

ecommendations: o The EC should be fully transparent about what the mini-ID wallet will achieve in terms of data protection goals and its expected timeline.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Encourages platforms to include transparent information on account processes, content standards, and to publish risk reviews with confidential redactions for external assessment.

Include information about: . The steps that users need to take from account creation to its deletion · Community guidelines that promote a positive, safe and inclusive atmosphere and that explain what conduct is expected and prohibited on their service, and what the consequences of non-compliance are.

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). Suggests platforms should explain both risks and benefits of registration to users for more informed engagement.

The NMA proposes to the following amendment: "Explain to users the risks and benefits of registration or why registration is necessary".

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Advocates for public transparency reports detailing risk review outcomes and preventive actions against inappropriate content for minors.

Public transparency reports from platforms detailing risk review outcomes and actions taken to prevent exposure to inappropriate content.

Ten recommendations to the European Commission to really protect children online (unknown). Insists on mandatory and timely disclosure of risk assessment reports in accessible, machine-readable formats to prevent concealment of risks by online platforms.

The guidelines currently do not include any requirements for platforms to publish their risk assessments and hence leave it up to Online Platforms to decide and potentially conceal risks.

WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers). Requests clarification on transparency responsibilities in marketing disclosures, emphasizing alignment with existing co-regulatory frameworks.

While Article 26 of the DSA provides a foundation for more transparent marketing, further clarification is needed on how disclosure responsibilities are shared across platforms, brands and content creators.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Recommends that risk reviews respond to external research and that platforms are transparent about risk mitigation measures considered but not implemented.

We further recommend including the need for risk reviews to respond to external research into platform risks to children's rights and encourage transparency on risk mitigation measures, which providers have considered, but not implemented, including a provider's reasoning.

CONCLUSION & POLICY DEMANDS (unknown). Demands mandatory, timely, and public disclosure of online platforms' risk assessments, advocating for independent child rights impact assessments.

The guidelines currently do not include any requirements for platforms to publish their risk assessments and hence leave it up to Online Platforms to decide and potentially conceal risks.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Emphasizes transparency in research access, public reporting of product experiments, and transparent rate limits to prevent misuse.

Despite digital platforms and AI companies' commitments to encourage third-party discovery of issues, many impose barriers that deter safety research.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Recommends open-source and prosocial licensing for platform transparency, requiring public disclosure of significant product experimentation results.

Some deliberative technologies are open-source by default, allowing for transparency in how decisions are facilitated, data is handled, and algorithms function.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Calls for research results involving minors to be made publicly and independently accessible, rejecting selective disclosure based on outcomes favorable to platforms.

In our view, such evaluation is a good start but it is insufficient. Continuous evaluation research with children is what is needed, and the results of such research need to be publicly available.

Ten recommendations to the European Commission to really protect children online (unknown). Reiterates the need for standardized, timely public disclosure of risk assessment by online platforms, alongside independent child rights impact assessments.

The guidelines currently do not include any requirements for platforms to publish their risk assessments and hence leave it up to Online Platforms to decide and potentially conceal risks.

Safe by Default (Panoptykon Foundation). Advocates for transparency and mitigation measures for algorithmic and recommender systems, highlighting the need for clear disclosure in content moderation.

On Risk Assessment and Mitigation for Algorithmic Systems",

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Argues that while platforms should consider publishing outcomes of Article 28 DSA risk reviews, results may contain sensitive information requiring caution.

However, the results of risk reviews often contain sensitive information.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Recommends caution in publishing risk review outcomes, stressing the balance between transparency and the protection of personal or commercial data.

While transparency may have certain benefits, it must be carefully balanced against the need to protect personal data and confidential commercial information.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Suggests periodic, detailed reporting by platforms to the Commission regarding measures for privacy and safety compliance for minors.

Should Very large Online platforms be required to submit to the Commission, on a periodic basis, a detailed report on the concrete measures adopted in compliance with the provisions set out in guideline sections 5, 6, 7, and 8 to ensure a high level of privacy protection, security, and safeguarding of minors.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Calls for greater transparency in the risk assessment process, including clarity on who was consulted and how mitigation measures address identified risks.

Bris also calls for the guidelines to more clearly highlight the transparency obligations regarding how the assessment has been conducted, who has been consulted, what risks have been identified and how the platform's proposed measures will mitigate those risks.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Recommends periodic communication to authorities of measures undertaken under the guidelines, advocating regular reporting for ongoing oversight.

Insert a recommendation concerning periodic reports to DSCs and the Commission on the concrete measures adopted in application of the recommendations in points 5, 6, 7, and 8 of the Guidelines themselves.

Policy_demands (unknown). Advocates for public, independently reviewed child safety impact assessments with regular reporting to ensure platforms prioritize children's safety above commercial goals.

Platforms should be obliged to submit child safety impact assessments which should be independently reviewed and made publicly available.

DOT Europe response1 (DOT Europe). Calls for alignment of notice quality requirements with DSA standards for precision and substantiation, referencing transparency obligations.

Similarly, the DSA sets out rules for sufficiently precise and adequately substantiated notices, therefore l. 775-776 should be amended in order to remain in line with the DSA text.

Consultation on DSA Art. 28 guidelines (The Danish Consumer Council (Forbrugerrådet Tænk)). Supports publishing risk reviews upon significant platform changes to enable external feedback, with a call for clearer definitions of 'significant change.'

However, making providers publish their risk review whenever they make significant changes to their platform, can give NGO's better understanding of the providers considerations, and enable timely feedback which could aid the general assessment of systemic risks.

Yoti_response_on_Article_28__2_.pdf (Yoti). Recommends transparency and regular auditing of age estimation methods, including sources, bias levels, and compliance with privacy requirements.

We would encourage that estimation approaches used must be transparent as to the source of data collected, in accordance with privacy requirements, the bias levels must be published transparently and independently audited, and must ensure that the data is instantly deleted.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Encourages companies to be transparent about ranking and recommender systems so experts can create safe usage guides for children and parents.

It is still important for companies to be as transparent as possible about how their ranking and recommender systems work, so that expert organizations can produce guides for children and parents to safely use the systems.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Suggests age-differentiated transparency with detailed guidance under the DSA regarding relevant information for minors.

Transparency requires an age-differentiated approach.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Urges platforms to provide up-to-date, empirical evidence on the effectiveness of child protection features and to publish findings for public scrutiny.

the best of our knowledge, there is insufficient research evidence as to the extent to which default features contribute to reducing the prevalence of a certain type of risk. For example, if a tagging or "stitching"12 feature is not available to a certain age group, does this lack of availability contribute to reducing children's experience of harassment or some other risk for that age group? Should the onus be on platforms to conduct research with children that would shed light on this issue and transparently publish findings of such research?

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Addresses issues of platforms withholding risk assessments by citing trade secrets, recommending public standardized disclosure.

Requirement: Public disclosure in standardized, machine-readable format

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT

(Adigital). Argues that DSA-required risk reviews should primarily be shared with regulators and researchers, because public disclosure could expose sensitive information.

However, the results of risk reviews often contain sensitive information.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Proposes immediate public risk assessment requirements and regular progress reporting to enhance accountability.

Public risk assessment requirement

Welke rol kunnen Telecom bedrijven spelen in de bescherming van kinderen in de online wereld? (KidsUnplugged). Promotes transparent, annual public reporting on a company's child protection measures and impact in the online world.

Transparante rapportage: Jaarlijkse publicatie over hoe het bedrijf kinderen beschermt en wat de impact is.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Criticizes self-regulatory approaches and calls for mandatory standards with real consequences, including public risk assessment requirements.

Only mandatory standards with real consequences will protect minors online.

Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus). Recommends platforms publish risk assessment results and create child-friendly versions to enable informed decisions by children and guardians.

providers should be encouraged to produce child-friendly versions of these reports to support transparency and empower children and their guardians with a clearer understanding of potential risks, enabling informed decision-making and appropriate behavioural responses.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Mandates publication of review outcomes regarding children's rights and insists on transparency for both processes and results to foster learning and accountability.

Mandate the publication of review outcomes. Platforms applying a child rights approach should make both their review process and results transparent and accessible. Public disclosure fosters accountability and facilitates sector-wide learning. It enables regulators, researchers and civil society to monitor whether children's rights are truly upheld.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Promotes 'transparency by design' as a foundational principle, ensuring all platform interactions and data requirements are clear and comprehensible.

In general, we understand transparency by design as the commitment to making all points of interaction with technology, as well as data input requirements, clear and comprehensible.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Supports robust transparency measures for minors in line with similar legislative proposals, commending the Commission's emphasis on the issue.

Common Sense Media also commends the Commission for placing such an emphasis on transparency in the guidelines.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Urges mandatory transparency and external accountability mechanisms for public oversight, recommending layered disclosure methods including accessible iconography.

Without mandatory transparency measures and external accountability mechanisms, governance structures risk operating without meaningful public oversight, limiting their effectiveness and undermining public confidence in platform child protection efforts.

Feedback DSA (unknown). Requests clarification on whether age estimation methods should be transparent and how their evaluation is conducted and by whom.

Should Age estimation methods be made publicly transparent?

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Advocates for greater transparency specifically in AI-powered chatbots interacting with minors.

chatbots (agents conversationnels personnifies) fonctionnant par intelligence artificielle (IA) plus transparents

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Calls for child-readable transparency reports on content moderation, AI, and age assurance, and public tracking of metrics like re-upload rates for flagged content.

Mandate child-readable transparency reports on moderation practices, Al usage, and age assurance measures.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Demands public disclosure of risk assessments by all platforms in standardized formats with specified reporting timelines.

Requirement: Public disclosure in standardized, machine-readable format

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Proposes that trusted news outlets be prioritized and visibly indicated on platforms to support minors' access to reliable information.

To ensure the right to information focusses on real information, we recommend online service providers prioritising trusted news outlets and making it visible – e.g. with a virtual badge – that a news outlet is for example well established and adheres to the laws and journalistic codes of conducts of the respective country.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Recommends app store operators provide information on average and individual spending for greater cost transparency for minors.

App-Store Betreiber als zentrale Akteure bei der Abwicklung von Transaktionen im Mobile Gaming klare Informationen über die durchschnittlichen Kosten eines/einer (aktiven) Nutzers/Nutzerin dieses Spiels anbieten sowie jedem/jeder Spieler:in individuell Informationen über seine/ihre bisherigen Gesamtausgaben in einem Spiel zur Verfügung stellen.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Advocates for public risk review publication after significant changes, with clear criteria and information accessible to minors.

Accountability through transparency is a key goal of the DSA - we therefore welcome that the guidelines have included the possibility for online platforms to publish the outcomes of their risk reviews in section 5 and suggest that the language be strengthened.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Cautions against public disclosure of risk reviews due to sensitive information, proposing sharing only with authorities and vetted researchers.

We therefore recommend that the outcomes of these risk reviews should, at most, be made available by providers of online platforms to the authorities competent to supervise the provider's compliance with the DSA and vetted researchers under Article 40(4) of the DSA.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Calls for accessible information for children about trusted flaggers and detailed, individual transparency on app expenditures in gaming.

Um diesem Problem zu begegnen, müssten App-Store-Betreiber als zentrale Akteure bei der Abwicklung von Transaktionen im Mobile Gaming klare Informationen über die durchschnittlichen Kosten eines/einer (aktiven) Nutzers/Nutzerin dieses Spiels anbieten sowie jedem/jeder Spieler:in individuell Informationen über seine/ihre bisherigen Gesamtausgaben in einem Spiel zur Verfügung stellen.

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 (European Commission). Emphasizes that all necessary platform functioning information should be accessible to minors, and changes to terms or policies should be logged and published for transparency.

In view of minors' developmental stages and evolving capacities, additional considerations concerning the transparency of an online platform's functioning are required to ensure compliance with Article 28(1) of that Regulation.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Requests clarification on mechanisms for platforms to acknowledge minors' presence through credible third-party evidence, influencing transparency practice.

As currently phrased, the examples are limited to situations where the provider processes relevant personal data or has conducted or commissioned its own research on whether minors access their platforms.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Calls for periodic publication of risk assessment reports and understandable information on algorithmic moderation and recommendation systems.

Le rapport devra faire l'objet d'une publication périodique sur le modèle du rapport d'analyse de risques auxquels sont soumises les très grandes plateformes au titre de l'article 35 du DSA.

Ten recommendations to the European Commission to really protect children online (unknown). Insists on standardized, accessible public disclosure of risk review assessments and independent child rights impact assessments.

The guidelines currently do not include any requirements for platforms to publish their risk assessments and hence leave it up to Online Platforms to decide and potentially conceal risks.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Proposes that platforms ensure the use of high-quality, representative datasets for algorithmic systems as part of their transparency and governance framework.

In compliance with Articles 28 and 34 of the Digital Services Act, platforms should affirm that high-quality, representative datasets are used in all algorithmic systems accessible to minors, as part of their transparency and governance framework to mitigate systemic risks, prevent discriminatory outcomes and ensure compliance with EU fundamental rights obligations, including the rights of the child.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Stipulates transparent reporting and easy-to-use complaint mechanisms, particularly for parental control and user reporting features.

In addition, they have to put in place transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints in relation to flagging and reporting and parental control systems.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Mandates that risk assessment testing results for large platforms be included in reports, independently audited, and use quantifiable rather than self-reported metrics.

The tests should use metrics that demonstrate quantifiable effects, not self-reporting of having done testing.

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). Argues that not all transparency-related information should be in terms and conditions, and that transparency measures should be tested before being made mandatory.

While LinkedIn recognises the value in making much of this information public-facing and readily accessible to its members, in most (if not all) instances LinkedIn's terms and conditions are not the appropriate place to surface such information.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Requests reconsideration of duplicative requirements for logging and publishing all changes to terms and conditions for minors, noting existing compliance processes.

Inform all impacted users of significant changes to terms (Art 14(2))

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Supports robust transparency and technical reporting guidelines, including data points for verification and compliance auditing.

There should be a reporting requirement that captures information such as fraudulent accounts, security issues, verification problems as well as other relevant data points that can be used for verification and auditing compliance with the guideline requirements.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Supports greater transparency for virtual currency use and requires justification and publication of platforms' risk review assessments.

To ensure that the risk review is effective, we call for transparency, i.e. platforms should be required to publish their risk reviews and to clearly justify their assessment.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Mandates timely public disclosure of risk assessments in machine-readable formats and calls for independent impact assessment to prioritize child safety.

The guidelines currently do not include any requirements for platforms to publish their risk assessments and hence leave it up to Online Platforms to decide and potentially conceal risks.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Advocates for providers of age assessment systems to communicate in transparent and child-friendly ways about data practices, procedures, and user rights.

The respective measure should also be explained transparently and in a manner appropriate to the target audience, e.g., in language suitable for children and young people, so that they are empowered to make an informed decision about the chosen procedure on this basi

How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition). Highlights the transparency gap between traditional and digital media, emphasizing the importance of measurement and public reporting for effective DSA enforcement.

We believe that recognizing and accounting for this asymmetry and transparency gap is necessary as the gap in the enforcement of the DSA is critical as it could jeopardize the monitoring and enforcement that is necessary to achieve the objectives of the draft guidelines, particularly when it comes to age verification.

European Commission Article 28 Guidelines Feedback (unknown). Recommends transparency in aggregate data about minors' time spent online and the effectiveness of related management tools, ensuring privacy.

There should be meaningful transparency in aggregate (so that it is privacy preserving) about the distribution of time spent by teens, and the effectiveness of time management tools.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Warns that transparency and information provision alone do not suffice for adequate minor protection without additional measures.

Es sollte insbesondere klargestellt werden, dass Transparenz oder das Bereitstellen von Informationen als Maßnahme alleine nicht ausreichend ist, um einen hinreichenden Schutz von Kindern und Jugendlichen sicherzustellen.

1.4.6 Oversight, Monitoring, and Accountability

The category 'Oversight, Monitoring, and Accountability' in the context of the Digital Services Act (DSA) emphasizes the need for rigorous, independent oversight and ongoing monitoring of online platforms, especially concerning the protection of minors. Across the collected insights, a strong consensus emerges that self-regulation and internal assessment alone are insufficient to ensure children's safety and that independent, expert-led oversight mechanisms—such as audits, external reviews, and public reporting—are vital. Many contributions highlight the importance of regular, transparent evaluation processes, including systematic risk assessments, the participation of relevant stakeholders (such as civil society, researchers, and child rights organizations), and clear reporting intervals to enhance accountability and adaptability to evolving risks. Notably, the insights advocate for the establishment of dedicated oversight bodies with powers of audit, intervention, and sanction, often recommending that such bodies be composed of multidisciplinary experts and funded in a manner that ensures their independence. There is a notable call for platforms to document and archive their decision-making, provide meaningful data and metrics, and ensure that both direct and indirect societal harms are identified and mitigated. The necessity of involving independent experts in risk reviews, ensuring continuous due diligence, and adopting transparent monitoring methods are recurrent themes. Overall, the collective knowledge promotes a robust, transparent, and multi-layered governance framework to guarantee platforms are held accountable for safeguarding minors under the DSA.

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments. (Ten recommendations to the European Commission to really protect children online (unknown))

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Evaluation mechanisms should include independent assessments as good practice, and arguably it should be a requirement for "high risk" services. (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))

External review is necessary to introduce a verification layer that strengthens both compliance and public trust. (CONCLUSION & POLICY DEMANDS (unknown))

ort-term (3-6 months): · Independent oversight body establishment (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))

External review is necessary to introduce a verification layer that strengthens both compliance and public trust. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Highlights the importance of maintaining regulatory oversight of user traffic to avoid pushing users towards less regulated and harder-to-monitor sites, which would undermine child protection efforts.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Calls for independent oversight in risk assessments and emphasizes that self-regulation is insufficient, especially when commercial interests are at play.

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments.

Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)). Recommends the establishment of monitoring and review mechanisms post-implementation, involving SMEs, civil society, and national authorities to continually assess and update policies.

Establish monitoring and review mechanisms: After implementation, a structured review process involving SMEs, civil society, and national authorities should evaluate impact and inform future updates.

Ten recommendations to the European Commission to really protect children online (unknown). Stresses the need for independent review and public availability of child safety impact assessments to ensure platforms prioritize child safety over commercial interests.

Platforms should be obliged to submit child safety impact assessments which should be independently reviewed and made publicly available.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Advocates for comprehensive, ongoing due diligence, ensuring dynamic review of risks to children's rights and continuous transparency and accountability in platforms' operations.

whilst it is important that due diligence, including child rights impact assessments, are carried out when any significant changes are made to a provider's online platform, it is also important that due diligence, including assessing for risks to children's rights, is carried out in an ongoing way even when major changes are not made to the platform.

CONCLUSION & POLICY DEMANDS (unknown). Supports the establishment of independent oversight mechanisms for verifying the accuracy and completeness of risk assessments, instead of relying solely on self-regulation.

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Recommends shifting accountability to platforms through product liability for societal harm and calls for audits and transparency to address large-scale digital risks.

Codifying product liability for the adverse social impacts of platform design is essential to reducing digital harm because it shifts accountability from individual users and content moderation to the systemic design choices that drive large-scale societal risk.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Proposes mandating democratic oversight, transparency, and independent audits for foundational governance of platform research and operation.

B1. Mandate Democratic Platform Oversight, Transparency, and Audits

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Welcomes effective monitoring and evaluation, suggesting more concrete requirements for platforms, including continuous research with minors and assessment of moderation.

Continuously conduct research with minors of diverse backgrounds whose goal is to evaluate the effectiveness of a variety of systems available to them, including the effectiveness of moderation systems

Ten recommendations to the European Commission to really protect children online (unknown). Reiterates the necessity for independent oversight in platform risk assessments to adequately protect children online.

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Requests clarification on how new monitoring and governance obligations for online minors' safety intersect with existing DSA articles, to avoid duplicative oversight.

It is unclear whether such measures are in addition to risk review obligations (Section 4, 5 and 10), the above-mentioned governance measure in Section 8.1 and for VLOPs Compliance Office functions and Art. 34, 35 and 41 DSA.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Critiques platforms being solely responsible for violation determinations, highlighting discrepancies between children's experiences and platform assessments, and calls for involvement of independent experts.

Bris also finds it problematic that platforms alone are responsible for determining whether a violation on their platform has occurred.

DOT Europe response1 (DOT Europe). Suggests greater clarity is needed on the required frequency and extent of internal audits, reviews, and reports concerning minors protection under DSA guidelines.

To support compliance with the monitoring and evaluation obligation, the Guidelines could provide further clarity regarding the frequency and extent of required internal audits, reviews, and reports related to minors protection measures.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Recommends platforms provide data and clear governance processes for handling user reports from children to ensure responsiveness and accountability.

As such, platforms should provide metrics as to how often user reports from children are not actioned and their governance processes to ensure they are giving proper deference to children when they encounter content they find problematic.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Suggests confidential risk review submissions to supervisory authorities and setting clear timelines for required monitoring and evaluation.

Relevant providers of online platforms should confidentially submit their risk reviews to the competent supervisory authorities (while maintaining the provider's significant business secrets, which are to be excluded from this).

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Argues for independent assessments as a requirement in evaluation mechanisms, particularly for high-risk services, to enhance the reliability of oversight.

Evaluation mechanisms should include independent assessments as good practice, and arguably it should be a requirement for "high risk" services.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Recommends the formation of an independent oversight body with multi-disciplinary experts, capable of conducting audits, mandating changes, and imposing sanctions.

Powers: Conduct audits, mandate changes, impose sanctions

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Proposes the establishment of an independent oversight body as a near-term priority in strengthening protection for minors online.

Independent oversight body establishment

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 (BeSmartOnline! Maltese Safer Internet Centre). Highlights the need for defined timelines and clear criteria for risk reviews of mid-sized platforms to address framework vulnerabilities.

The absence of clear timelines for risk reviews outside the scope of VLOPs and VLOSEs represents a vulnerability in the framework.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Emphasizes setting precise, reasonable deadlines for risk reviews on non-VLOP platforms to ensure sustainable child protection systems.

This is a crucial step in ensuring the sustainability of online child protection systems, as reviews of the risks generated by online platforms do not benefit from a clear temporal framework, with the exception of VLOPs and VLOSEs.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Recommends open APIs for trusted flaggers and minimum risk assessment update intervals for platforms above significant audience thresholds to improve oversight efficiency.

the Association e-Enfance/3018 recommends that platforms be required to provide open and documented application programming interfaces (APIs), enabling trusted flaggers-such as the 3018 helpline-to automate the submission of reports using their own tools.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Stresses the necessity of independent oversight and clear obligations, rather than leaving minors' protection to platforms' or institutions' discretion.

The protection of minors cannot depend on the goodwill of profit-driven platforms or the competence of under-resourced institutions. It requires clear obligations, independent oversight, and personal accountability for those who fail our children.

Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus). Suggests requiring risk reviews at least every six months and enhancing external oversight and transparency in risk review processes.

We recommend amending this provision to require a minimum review frequency of every six months, in addition to the existing trigger for platform changes.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Calls for clearer risk review obligations, continuous monitoring, and independent Child Rights Impact Assessments with periodic public reporting.

Clarify the concept of "significant changes" and explicitly state that review must be a continuous process and not a one-time obligation.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation).

Advises against sole reliance on provider-driven assessments and advocates encouragement of independent expert involvement in evaluating services and mitigation measures.

e recommend that the Commission specifically encourage platforms to seek input from independent researchers and experts in evaluating, among other aspects, whether a service or part thereof is accessible to minors, the effectiveness of age assurance methods, the assessment of risks and the effectiveness of mitigation measures, whether transparency declarations regarding terms and conditions, and commercial communications are understandable and age-appropriate for children.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Advocates for public change-logs, proportional external oversight, and mechanisms for tracking the impact of platform changes on child safety.

Documented "adjust-and-prove" loop: require a public change-log showing each design adjustment, the trigger (consultation, incident data, research) and the measurable effect after N days.

Statement - DSA Guidelines (Protect Children). Supports independent oversight mechanisms, including regular audits of online platforms to ensure continuous refinement of safety standards for minors.

Establish independent oversight mechanisms and regular audits of online platforms.

Feedback DSA (unknown). Emphasizes the continued involvement of academic researchers in monitoring and evaluation of platform governance to uphold DSA compliance.

Given that many of these guidelines are grounded in academic research, the continued involvement of researchers in monitoring and evaluation is essential.

Comments of Slovak DSC to the EC Guidelines on Protection of Minors (Slovak Digital Skills Coalition). Proposes requirements for platforms to document and archive decision-making, facilitating regulatory oversight in accordance with DSA principles.

A requirement should be introduced to document and archive decision-making for the purposes of regulatory oversight.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Welcomes regular independent audits of safety and privacy settings on platforms, along with reporting to Digital Services Coordinators (DSCs).

e welcome the call for digital services to: · Mandate regular independent audits of safety and privacy controls, with reporting to Digital Services Coordinators (DSCs).

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Suggests an independent oversight body funded by platform fees and empowered to audit, mandate changes, and impose sanctions.

Powers: Conduct audits, mandate changes, impose sanctions

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Recommends audits, expert consultation, and ongoing monitoring for early detection and timely intervention in cases of problematic usage patterns among minors.

Ohne kontinuierliches Monitoring bleiben problematische Entwicklungen (z. B. Zunahme zwanghafter Nutzung) unentdeckt und kann daher nicht oder nicht rechtzeitig gegengesteuert werden.

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 (European Commission). Details roles and oversight structure for trusted flaggers and highlights the requirement for systematic data gathering on risks, with senior management reporting.

The trusted flagger status is awarded by the Digital Services Coordinator of the Member State where the entity is established, provided that the entity has demonstrated their expertise, competence, independence from online platforms, as well as diligence, accuracy and objectivity in submitting notices.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Criticizes sole reliance on platform self-assessment of minors' risks, noting that it often leads to prioritization of business interests over safety.

We find it problematic that it is the provider of the online platform which solely evalu- ates and assesses the risk.

Ten recommendations to the European Commission to really protect children online (unknown). Reiterates the call for independent oversight to validate the accuracy and thoroughness of platforms' risk assessments for children.

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Argues for independent oversight and structured governance frameworks beyond self-directed monitoring, together with mandatory annual risk reviews and public disclosure.

Monitoring is entirely self-directed with no mechanism for independent oversight or audits except for VLOPs.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Suggests requiring very large platforms to provide periodic public reports to the Commission on implemented measures safeguarding minors.

Should Very large Online platforms be required to submit to the Commission, on a periodic basis, a detailed report on the concrete measures adopted in compliance with the provisions set out in guideline sections 5, 6, 7, and 8 to ensure a high level of privacy protection, security, and safeguarding of minors.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Focuses on monitoring and evaluating the broader market impact of the DSA, particularly regarding competition among digital services.

Mukherjee, Supantha, and Foo Yun Chee. "Exclusive: EU's new tech laws are working; small browsers gain market share." Reuters, April 10, 2024.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Urges regular mandatory audits and transparency of recommender systems to prevent exposure of under-18s to illegal and harmful content.

We strongly urge the Commission to extend regular mandatory audits and transparency of algorithmic recommender systems to ensure they do not promote illegal and harmful content to under 18s.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Calls for external expert oversight and transparent publication of risk assessments, as well as appointing dedicated personnel for safety oversight.

However, it is essential that these reviews are qualified by external experts and child rights organizations.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Advises maintaining research integrity by managing conflicts of interest between industry and scientific research, advocating for transparency in researchers' earnings.

We roepen daarom ook op om van onderzoekers in dit veld te eisen dat zij hun inkomsten openbaar maken, zodat de integriteit van het onderzoek gewaarborgd blijft.

On the concept of personal integrity in the german protection of minors (unknown). Describes a model where providers choose precautionary measures subject to regulatory oversight, encouraging flexibility while ensuring compliance.

The legislator leaves it up to the services to independently decide which precautionary measures they consider to be meaningful and effective for countering specific risks and dangers in their services or on their platforms.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Supports designating a dedicated individual or team with accountability for children's privacy, safety, and security on the platform.

Save the Children fully supports the provision to assign to a dedicated person or team the responsibility for ensuring a high level of minor's privacy, safety and security.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Restates the need for independent oversight to ensure risk assessments are accurate and not influenced by commercial self-interest.

Establish independent oversight, which is necessary to ensure the accuracy and completeness of risk assessments.

How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition). Recommends using independent audience measurement as a monitoring tool to verify age verification and understanding minors' digital media consumption.

We recommend that the Commission duly considers independent audience measurement as an enforcement monitoring tool and mechanism without which we predict challenges in verifying the actual efficiency of age verification mechanisms or monitoring attention over-extraction.

European Commission Article 28 Guidelines Feedback (unknown). Advocates independent auditing and testing of minors' safety features, including establishing metrics to track harms and youth agency over time.

Independent auditing and testing of: the safety of youth on the platform, the resilience of safety features, and to evaluate feedback and reporting tools.

1.4.7 Regulatory Integration and Governance

The collected insights within this category emphasize the necessity of comprehensive, rights-driven, and harmonized regulatory frameworks for digital service governance, particularly under the EU Digital Services Act (DSA). Key themes include the alignment and integration of various risk assessment and compliance requirements across DSA provisions and other national/international legal instruments (such as AVMSD, NIS2, and GDPR). Many contributions stress the importance of transparency, pluralistic governance, and coordination among regulatory bodies to avoid duplication and fragmentation. There is consensus on tailoring governance both to local contexts and across sector-specific needs, while maintaining cohesion and clarity in obligations—especially surrounding the protection of minors, content moderation, and privacy. A notable trend is the call for recognizing equivalent compliance across borders (e.g., acknowledging risk reviews performed under the UK's Online Safety Act), and the recommendation that guidelines explicitly address overlaps, reference sectoral and national laws in guideline texts, and facilitate systemic cooperation between various authorities (e.g., Digital Services Coordinators, EDPB). Additional recommendations highlight the role of documented governance policies, senior management accountability, and the institution of dedicated child safety officers as part of effective oversight. Special attention is given to educational technology platforms, advocating for them to be held to similar rigorous standards as social platforms.

Requirements for risk review need to be aligned with the general framework of due diligence and risk assessment obligations already established by the Digital Services Act. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

We welcome the integration of Article 28 risk reviews into the broader systemic risk assessments for VLOPs (Articles 34 & 35 DSA). (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))

Once again, it is important to ensure proper coordination between the Article 34 DSA risk assessment and the Article 28 DSA impact assessment. (Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University))

Anu Bradford outlines three major paradigms of tech governance: the US market-driven model prioritizing innovation and corporate freedom, the Chinese state-driven model focused on control and surveillance, and the EU rights-driven model emphasizing content moderation, privacy, and human dignity. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

For this framework to be considered due diligence, it must be materialized in pre-approved and documented policies and processes, which are periodically reviewed as part of a continuous improvement process. (COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation))

However, due to the fundamentally different nature of online search engines, the direct relevance of the Guidelines to their operations will likely be considerably lower. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Advocates for adopting EU rights-driven tech governance, emphasizing transparent regulation and the integration of content moderation, privacy, and dignity under the DSA.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Stresses the need for rights-driven legal frameworks and locally adapted, pluralistic governance in digital services regulation with stringent antitrust enforcement.

Global civil society promotes stringent antitrust laws and corporate responsibility measures to curb monopolistic practices and encourage more equitable, prosocial digital environments necessary for democracy and human rights.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Calls for holistic integration of Article 28 with other DSA provisions, including child-friendly design and clear cross-article implementation guidance.

Article 28 should be implemented synergistically with other DSA provisions to create a comprehensive child protection ecosystem.

Ten recommendations to the European Commission to really protect children online (unknown). Urges application of DSA risk and security standards to edtech platforms, due to their similar risk profiles to social platforms and history of inadequate oversight.

Educational technology platforms, widely used in schools - including digital workspaces to connect schools with students and parents widely used upon schools'input - should be subject to the same risk assessment standards and security requirements - right from the design stage - as social platforms.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Recommends aligning risk review requirements with existing DSA due diligence frameworks and prioritizing standards for age-appropriate online service design.

Requirements for risk review need to be aligned with the general framework of due diligence and risk assessment obligations already established by the Digital Services Act.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Supports consistent application of Article 28 and recommends individual references to all relevant sector-specific obligations in the DSA guidelines.

As mentioned above, the Media Board welcomes the draft guidelines on the protection of minors as proposed by the European Commission and wishes to express its support to the measures suggested in view of the consistent application of article 28 of the DSA. However, with this contribution we encourage the Commission to add all the individual reference to sector specific obligations related to VSPs, instead of referencing only some of them in the footnotes

DOT Europe response1 (DOT Europe). Advocates for clarifying how different legal instruments overlap and suggests the Guidelines should explicitly address interplay between various regulations covering online platforms.

The Guidelines and accompanying communications could have been an opportunity to clarify the interplay between different legal instruments that regulate different subsets of online platforms, e.g. AVMSD, EMFA, GDPR, among others, eve

DSA_Article_28_GitHub_Response (GitHub). Encourages alignment of DSA risk assessment obligations with international frameworks to streamline compliance for global platforms.

We also encourage alignment with other international regulatory frameworks which require risk assessments to promote consistency and efficiency for platforms operating across jurisdictions.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Requests detailed clarification on the interaction between Article 14(3) and Article 28 DSA, including explicit explanation of relevant terms.

To avoid misunderstandings, the relationship to Article 14(3) DSA should be described in more detail.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Welcomes integration of Article 28 risk reviews with broader systemic risk assessments for Very Large Online Platforms to streamline and avoid duplication.

We welcome the integration of Article 28 risk reviews into the broader systemic risk assessments for VLOPs (Articles 34 & 35 DSA).

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Advises coordinated action between the Board of Digital Services Coordinators and other relevant bodies to prevent conflicting regulatory guidelines.

we strongly advise the Board of Digital Services Coordinators to act in concert with other bodies (e.g., EDPB) as there is a risk to produce guidelines that might conflict with future guidelines or opinions.

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Proposes aligning governance frameworks with NIS2 cybersecurity schemes, assigning strategic and implementation responsibilities to management and senior management.

It is advisable that the governance framework be aligned with the scheme established for cybersecurity in NIS2: management bodies should be responsible for approving the strategy and overseeing its implementation, while senior management should be responsible for execution.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Highlights

the importance of mandatory, enforceable governance provisions such as the assignment of dedicated child safety officers with direct oversight.

As stated earlier in this document, the use of "should" rather than "must," significantly undermines the enforceability of essential governance provisions.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Identifies fragmentation in DSA oversight and calls for clearer, harmonized risk review frameworks to safeguard fundamental rights consistently across the EU.

This fragmentation may be further aggravated by the fact that the conceptual framework of the Risk review is itself in need of further clarity, but also the fact that DSA oversight and enforcement at national level is taking place at various speeds and levels of effectiveness.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Recommends clarification regarding whether and how Article 28 DSA Guidelines apply to search engines as opposed to online platforms.

Article 28(1) DSA applies to providers of online platforms, and not to online search engines.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Encourages recognition of equivalent regulatory compliance from frameworks like the UK's Online Safety Act to streamline business obligations.

That being said, we believe that a recognition of equivalent compliance efforts - notably in the context of the UK's Online Safety Act - would contribute towards the Commission's overarching goal of simplification and streamlining for businesses.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Recommends more explicit references to AVMSD and national laws in the main DSA guidelines text for a coordinated minor protection approach.

An explicit reference both the AVMSD and to such relevant national laws could allow a coordinated and comprehensive approach to minor protection.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Suggests further alignment of DSA Article implementation approaches to link upstream design for minors with measureable transparency and protection outcomes.

Our response recommends that the European Commission continue to work to further align implementation approaches across DSA Articles into a more cohesive whole that links upstream design considerations for minors with verifiable metrics and robust transparency.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Argues for allowing use of assessments made under comparable non-EU regulations when relevant for DSA compliance.

Platforms should be allowed to leverage existing assessments conducted under comparable regulations, such as the UK's Online Safety Act, where relevant and applicable.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Insists that edtech platforms in schools be subject to DSA-standard risk and security requirements in light of their wide use and inherent risks to minors.

Educational technology platforms, widely used in schools - including digital workspaces to connect schools with students and parents widely used upon schools'input - should be subject to the same risk assessment standards and security requirements - right from the design stage - as social platforms.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Calls for clear explanation and coordination between Article 28 and risk/impact assessments in Articles 34 and 35, due to their overlapping roles in minor protection.

Once again, it is important to ensure proper coordination between the Article 34 DSA risk assessment and the Article 28 DSA impact assessment.

1.4.8 Stakeholder Engagement and Collaboration

Stakeholder engagement and collaboration are central to effective risk assessment, transparency, and oversight in the implementation of minors' protection guidelines under the Digital Services Act (DSA). Insights from the documents emphasize the importance of multi-stakeholder involvement, including children, parents, civil society organizations, experts (e.g., psychologists, technical specialists), educators, industry actors, and regulators, at various stages of policy design, risk assessment, and mitigation. Calls are made for not just consulting these groups but actively integrating their insights into decision-making, ensuring participatory approaches—especially in risk reviews and development of measures—and making outcomes transparent and accountable. Collaborative mechanisms, such as research facilitation and operational partnerships, are spotlighted to build a robust evidence base and ensure that both technological and social realities are reflected. There is a significant focus on international and cross-sectoral cooperation, leveraging knowledge from diverse regulatory, academic, and industry sources to tackle global challenges such as age assurance, online safety ratings, and platform moderation. Recommendations span from funding interdisciplinary research and establishing multistakeholder governance bodies, to clear documentation and public reporting on how stakeholder input shapes regulatory decisions. Ultimately, the documents advocate for continuous and structured engagement through dialogue, transparency, and shared responsibility, fostering trust and adaptive responses to emerging risks in the online environment for minors.

We therefore recommend adding to the guidelines that providers, in light of their risk review, should consult children, guardians, educators and their representative organisations. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

It is crucial that the guidelines explicitly encourage the involvement of child rights and development experts considering their expertise in identifying risks and considering all impacts on children including unintended consequences of proposed changes. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Moreover, strong global collaboration among regulators, civil society, and the tech industry is particularly crucial in addressing common pain points, such as age assurance, which can help enforce child safety policies effectively. (Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media))

Support Infrastructure for Independent Research and encourage the creation of shared tools, datasets, and secure sandboxes to facilitate rigorous, transparent AI safety evaluations by independent experts. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Promote stronger dialogue between regulators and digital service providers, to ensure that implementation trajectories reflect technological and economic realities. (Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS))

Such an assessment is important because it ensures that any restriction to the exercise of fundamental rights and freedoms is proportionate, and should be done in consultation with experts and children. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

EFPA contribution to consultation on the protection of minors guidelines (European Federation of Psychologists' Associations (EFPA)). EFPA advocates for explicit calls to facilitate research on online impacts for minors and for platforms to enable researcher access to anonymized data, supporting open science and evidence-based policy.

It could also suggest that the Commission or Member States explore mechanisms to facilitate researcher access to appropriately anonymised and aggregated platform data for such research, adhering to open science principles and data protection regulations.

OFFLIMITS (Stichting Offlimits). OFFLIMITS highlights the value of strong operational partnerships between trusted flaggers, authorities, and civil society at national and international levels to address online harms collaboratively.

This strong operational capacity is further supported by long-standing and trusted partnerships Offlimits have built with national stakeholders, including the National Police, public prosecutors, governmental authorities and other key civil society organisations active in the field.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild recommends that proportionality and risk assessments under the DSA involve direct consultation with children and experts to balance regulatory interventions and protect rights.

Such an assessment is important because it ensures that any restriction to the exercise of fundamental rights and freedoms is proportionate, and should be done in consultation with experts and children.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). The Council on Technology and Social Cohesion underscores the need for multistakeholder governance and financial incentives to promote prosocial tech development, ensuring broad investor and institutional engagement.

To better incentivize fund managers to invest in prosocial tech, policymakers, and philanthropic actors should establish blended finance mechanisms-such as public-private co-investment funds, risk guarantees, or outcome-based grants-that reduce the financial risk of investing in socially beneficial technologies.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). A call for supporting independent research infrastructure and recognizing the accreditation hurdles faced by nonprofits, especially from the Global South, to ensure responsible AI regulation and inclusive participation.

It is important to recognize the challenges nonprofits (especially from the Global South) face in accreditation systems.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). CDT Europe encourages strengthening civil society and expert involvement in the guidelines for risk assessment and mitigation, building on existing references to international frameworks.

CDT Europe welcomes the references to resources by the UN, the OECD and Member States throughout the guidelines. At the same time, we would welcome further emphasis on the knowledge and expertise developed by civil society organisations, including in how international legal frameworks should be interpreted and enforced.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). WebGroup Czech Republic argues that effective regulation should be evidence-based and involve industry, cautioning against approaches that over-rely on websites being responsible without broad collaboration.

WGCZ supports the better regulation of online services and believes in the value of building on foundational developments drawing genuine online safety benefits across the online environment.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). AIR MEDIAS SAS calls for sustained dialogue between regulators and digital service providers to ensure guidelines are practical, technically informed, and reflect industry realities.

For platforms, committing to this path involves strategic and resource-intensive decisions, which cannot be made without greater clarity on how these efforts will be assessed by regulatory authorities.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). The document pushes for enhanced transparency and accountability by documenting and communicating how stakeholder participation informs policy outcomes.

ountability: o Document how input influenced decisions

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Advocates for increased funding and dissemination of research to inform stakeholders and enable evidence-based policymaking for child safety online.

Fund More Research.202 There are many unanswered questions about how the Internet impacts minors (both positively and negatively), especially with respect to niche subpopulations.203 The government could fund more research into these issues to lay a proper foundation for evidence-based policymaking.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Common Sense Media underscores the necessity of global collaboration among regulators, civil society, and industry to tackle child safety challenges, such as age assurance.

Moreover, strong global collaboration among regulators, civil society, and the tech industry is particularly crucial in addressing common pain points, such as age assurance, which can help enforce child safety policies effectively.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis champions sharing moderation procedures and policies with civil society for feedback and independent bias testing.

Share the policies and procedures with civil society groups in order to show how a platform moderates its content in order to gather feedback from other specialists or independent experts.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). COFACE Families Europe recommends involving children, guardians, educators, and their representatives in DSA risk reviews and calls for their publication to support transparency.

We therefore recommend adding to the guidelines that providers, in light of their risk review, should consult children, guardians, educators and their representative organisations.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Highlights the importance of public accountability through reporting and disclosure on how stakeholder input is used in regulatory decisions.

Accountability: Public reporting to European Parliament

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Reiterates the emphasis on civil society expertise and the need to tailor engagement and compliance to platform capacities, especially for smaller online actors.

we would welcome further emphasis on the knowledge and expertise developed by civil society organisations, including in how international legal frameworks should be interpreted and enforced.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). CNCDH insists that civil society organizations and researchers must be closely involved in supervising platforms' obligations to protect minors' privacy, safety, and security.

La supervision du respect de l'article 28 du DSA, et donc de la manière dont les plateformes s'acquittent de leur obligation de garantir un niveau élevé de protection de la vie privée, de sûreté et de

sécurité des mineurs sur leur service, doit associer étroitement les organisations de la société civile ainsi que les chercheurs.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). The Hellenic Ministry of Digital Governance stresses explicit involvement of child development experts in DSA risk analysis to appropriately cover all potential impacts.

It is crucial that the guidelines explicitly encourage the involvement of child rights and development experts considering their expertise in identifying risks and considering all impacts on children including unintended consequences of proposed changes.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). The Safer Internet Centre Denmark urges the inclusion of trusted flaggers alongside other user support resources in guidelines to enhance public awareness of available support.

Regarding user support measures, we believe that the guidelines should also mention trusted flaggers along with the Safer Internet Centres and INHOPE, since it is important that the public become aware of all the support measures available to them

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). IEEE signals its commitment to bring technical expertise into collaborative regulatory processes, including codes of conduct and enforcement under the DSA.

IEEE SA stands ready to collaborate with European Union institutions, regulators and industry stakeholders to promote safe, ethical and age-appropriate digital ecosystems and would welcome the opportunity to contribute its technical expertise to upcoming delegated acts, co- regulatory codes of conduct, or further refinement of enforcement guidance under the DSA.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). PEGI illustrates international cooperation via age rating systems (e.g., IARC), promoting harmonized online safety standards through global collaboration with platforms and regulators.

PEGI s.a. co-founded IARC, the International Age Rating Coalition, which comprises rating boards from across the world, including PEGI and the USK in Germany, to provide an automated rating solution for the globalised market of apps, by which game publishers can obtain ratings for their game from all participating rating boards via a single application.

1.4.9 Vulnerable Groups and Special Protections

The collected insights highlight the necessity of specifically addressing the needs of vulnerable groups and ensuring special protections are embedded within risk assessments, transparency requirements, and oversight mechanisms for online platforms accessible to minors. Contributors emphasize that general child protection measures often overlook subgroups such as children with disabilities, those in poverty, LGBTIQ+ minors, and children outside family care, and thus risk assessments and safeguarding actions must be tailored accordingly. There is a call to adopt procedural, intersectional, and child-rights-based approaches across all digital policies, ensuring that children's voices and a range of their rights—including participation, privacy, protection, and non-discrimination—are systematically considered and operationalized, not merely acknowledged in principle. Further, multiple submissions recommend platforms perform detailed and ongoing risk assessments and impact evaluations for at-risk groups, considering cumulative harms and the influence of platform design on vulnerable children. The use of robust methodologies (e.g., long-term holdout experiments and disaggregated reporting) and independent reviews are suggested to ensure accountability and transparency. It's widely supported that regulatory frameworks should encompass coordinated, multi-stakeholder oversight—drawing upon the UN Convention on the Rights of the Child's broad principles—to ensure that protective measures remain current, data-driven, and equitable for all minors, particularly the most vulnerable.

Providers of online platforms accessible to minors should consider when applying measures under these guidelines the specific needs of children living in vulnerable circumstances, including children with disabilities, younger children, children living in poverty, children outside of family care, LGBTIQ+, among others. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

require assessment of cumulative harms, age-appropriateness, and impacts on vulnerable child groups. (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

Encourage platforms to disaggregate risks and consider how they impact vulnerable or marginalized groups of minors, aligning with UNCRC General Comment No. 25 (2021) on children's rights in the digital environment. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Children have challenges understanding whether AI-bots are real people. (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))

e recommend including a general principle that explicitly: · Recognises the best interests of the child as a procedural obligation, not just a value-based consideration; (SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands))

When releasing the results of long-term holdout experiments, the guidelines should clarify that platforms should report metrics for each of these at-risk populations. (European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute))

EFPA contribution to consultation on the protection of minors guidelines (European Federation of Psychologists' Associations (EFPA)). EFPA advocates for explicit, targeted risk assessments and tailored protections for minors with specific vulnerabilities, such as intellectual disabilities and neurodevelopmental conditions, beyond general accessibility mentions.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild stresses the importance of addressing the diverse needs of children in vulnerable situations—such as those with disabilities, in poverty, or lacking family care—when platforms implement child-protective Digital Services Act (DSA) requirements.

Providers of online platforms accessible to minors should consider when applying measures under these guidelines the specific needs of children living in vulnerable circumstances, including children with disabilities, younger children, children living in poverty, children outside of family care, LGBTIQ+, among others.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). The UCD Centre for Digital Policy recommends that platforms conduct risk assessments encompassing cumulative harms, age-appropriateness, and particular effects on vulnerable child groups.

require assessment of cumulative harms, age-appropriateness, and impacts on vulnerable child groups.

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Børns Vilkår highlights the unique risks faced by vulnerable and lonely children in their interactions with AI chatbots, underscoring the need for safeguards against technology that may inadvertently reinforce isolation.

hildren who feel lonely may experience not being seen, heard, or understood. When My AI steps in to fulfill some of these needs, it motivates more interaction, which can poten- tially lead the child to withdraw from other relationships and communities, thus not gaining experiences of succeeding in them. Consequently, the child's relationship with the chatbot can reinforce loneliness. The insistent manner in which My AI asks questions keeps the child engaged in the chat, which can further intensify loneliness.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). VIDEO GAMES EUROPE calls for guidance that reflects the full spectrum of children's rights as articulated in the UN Convention—not just a narrow focus on the child's best interests—in digital platform risk reviews.

The Committee also mentioned in this context the right to have equal and effective access to the digital environment, the need to protect children's right to life, survival and development and the right to be heard in matters that affected them.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). The European Board for Media Services recommends explicit recognition of overexposure and excessive use as risks, suggesting that only coordinated, complementary regulation can ensure true online safety for minors.

Explicitly include among the risks identified by the guidelines the issue of overexposure, that is, the extensive or excessive use.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). The USK submission urges a shift from arbitrary age-based thresholds to assessments grounded in actual risks to minors' well-being and integrity, when determining protective needs online.

Therefore, the focus should be solely on the actual risk of impairment or endangerment of the personal integrity of minors.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). This contribution calls for Child Rights Impact Assessments to be mandatory before launching features accessible to minors, carried out independently and with public disclosure of summary findings.

Public disclosure: Summary findings must be public

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Defence for Children - Netherlands proposes embedding a procedural child rights approach in DSA guidelines, centering systematic identification of affected rights, transparent trade-offs, and involvement of children and experts.

Anchors this obligation in a child rights approach, understood as a structured decision-making method grounded in children's rights, including: The systematic identification of rights at stake; The documentation of trade-offs made and their justification and the meaningful involvement of children and child rights experts.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis urges platforms to disaggregate risk evaluations, focusing specifically on the experiences of marginalized or vulnerable subgroups of minors, in line with the UNCRC's approach to digital rights.

Encourage platforms to disaggregate risks and consider how they impact vulnerable or marginalized groups of minors, aligning with UNCRC General Comment No. 25 (2021) on children's rights in the digital environment.

Feedback for 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 (xHamster). xHamster's feedback supports taking into account the full spectrum of children's rights—including participation, inclusion, and freedom of expression—when designing appropriate online safety measures.

Therefore, to ensure that measures to achieve a high level of privacy, safety and security for minors on an online platform are appropriate and proportionate, it is necessary to consider all children's rights, including their right to protection, non-discrimination, inclusion, participation, privacy, information and freedom of expression, among others."

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). The Knight-Georgetown Institute recommends platforms routinely run long-term holdout experiments to better understand and

improve the varied experiences of vulnerable subgroups of minors, with specific metrics and public data.

In their long-term holdout experiments, platforms should identify at-risk minor populations and oversample holdout groups for individuals with these characteristics.

1.4.10 Guidance and Continuous Improvement

The 'Guidance and Continuous Improvement' category captures a strong consensus on the need for dynamic, regularly updated guidance and oversight mechanisms for protecting minors online under regulatory frameworks like the DSA. Across numerous submissions, stakeholders call for periodic formal review of the guidelines—often emphasizing two-year cycles, with flexibility for earlier reviews in response to technological or societal changes. Many advocate for guidance to encompass evolving best practices, real-world experience, independent academic research, and state-of-the-art technological advances. Another recurring theme is the push for detailed, practical guidance, including concrete examples, clear criteria for risk assessments, and a systematic linkage between identified risks and mitigation measures. Contributors stress that the guidelines should not be overly prescriptive, instead facilitating flexibility so platforms can tailor solutions to their specific contexts while still meeting regulatory aims. The importance of inclusive, evidence-based reviews—involving national authorities, independent researchers, and affected stakeholders, especially children—emerges as crucial for ongoing relevance and effectiveness. Finally, transparency, documentation of compliance efforts, and continual improvements form a foundation for trust and accountability. Platforms are encouraged not only to test and refine measures before broad implementation but also to share findings and safety innovations. Such transparency, combined with good-faith efforts and open channels for feedback, ensures that the ecosystem keeps pace with emerging risks and advances in protecting minors online.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments. (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))

We encourage the European Commission to consider these guidelines as a living document, by establishing mechanism for regular review, to ensure that they remain relevant and effective. (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))

It is essential that the Commission continuously reviews the guidelines and adjusts as necessary. (Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)))

Some research finds content diversity can backfire. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Any content diversity process should therefore be tested. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

Public consultation on 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 (Coimisiún na Meán). Highlights the importance of child rights impact assessments (CRIA) within risk review processes and requests additional EU guidance and support tools for providers.

An Coimisiun also welcomes that the Commission may issue additional guidance or tools to support providers in carrying out reviews, including through specific tools for CRIA.

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). Calls for clearer and more elaborate guidance on risk mitigation expectations, especially as they relate to generative AI in online services under Article 28 of the DSA.

In general, the NMA recommends further elaboration and clarification of the expected risk mitigation efforts for online services that utilise generative AI tools, such as chatbots, assistants, and search functionalities.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Recommends a formal review of DSA guidelines two years after initiation to assure ongoing relevance amid rapid technological evolution.

In light of the rapid evolution of age assurance technologies, we also recommend a formal review of the guidelines two years after their commencement to ensure continued relevance and alignment with technological and societal developments.

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). Requests clarification on the legal grounds for further guidance on child rights impact assessments, seeking more precise regulatory references.

We would welcome clarification, at least by reference, regarding the legal basis for this future guidance.

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). Urges the provision of guidance to ensure transparency and human oversight, especially in the automated processing of personal data via smart contracts.

EDPB should offer guidance on ensuring transparency, contestability, and human oversight in smart contract deployments that process personal data.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Emphasizes pre-implementation testing of content diversity processes to avoid unintended negative consequences and promote evidence-based continuous improvement.

Any content diversity process should therefore be tested.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Advocates for continuous, transparent research on the efficacy of child protection measures, with findings made available to independent researchers for ongoing safety refinement.

Platforms should be required to conduct continuous, transparent research on the effectiveness of protective measures, with particular attention to diverse populations of children.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Suggests establishing a regular two-year review period for the guidelines, with the option for earlier review based on developments.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Recommends increased clarity in the DSA Draft Guidelines, particularly about intersections with other regulations and risk review procedures.

More clarity (in terms of intersection with other regulations; risk review; and certain :unselected: specifi

Safe by Default (Panoptykon Foundation). Encourages testing and refining safety measures on large platforms prior to full implementation to minimize unintended harms.

Therefore measures recommended in this briefing should be tested and refined before implementation.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Supports presenting the guidelines as a menu of best practices rather than as strict requirements, to preserve platform innovation and flexibility.

While detailed, the guidelines should be presented as a menu of best practices and examples, allowing platforms to choose solutions that fit their unique services.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Requests precise criteria and further guidance on when a service is considered directed at or predominantly used by minors for consistent DSA application.

Further guidance and clear criteria around "directed at" and "predominantly used by" in relation to, for example, the nature of a service, content, specific themes or elements that appeal to kids or teens, would be desirable as these assessments will determine whether the obligation laid down in Article 28(1) DSA applies or not.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Welcomes requirements for risk assessment updates after platform changes, and seeks examples clarifying what constitutes a significant change.

Bris sees a need for the guidelines to clarify-and potentially provide examples of-what constitutes a "significant change."

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Requests clarity over whether guideline measures, particularly age verification and parental controls, are sufficient under Article 35, and seeks transparency in compliance expectations.

The draft Guidelines state that implementing the recommended measures-whether partially or fully-would not, in itself, ensure compliance with the obligations of Very Large Online Platforms and Search Engines (VLOPSEs) under Articles 34 and 35 of the DSA (lines 93-99). This position creates uncertainty for providers:

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Advocates for flexible, transparent sharing of child safety solutions, allowing platforms to explain their methodologies publicly and accommodate innovation.

This way, platforms can explain how they are implementing safety features and why certain techniques are necessary to preserve their core product function.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Stresses continuous review and updating of guidelines with input from national law enforcement and stakeholders, and calls for clearer, more specific guidance in the DSA review process.

It is essential that the Commission continuously reviews the guidelines and adjusts as necessary.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Highlights the need for concrete connections between risk assessment and mitigation actions, and urges systematic mapping of risks to measures for clearer guidance.

From the USK's point of view, there is a particular lack of clear connection between risk assessment and specific measures to mitigate risk.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Suggests the guidelines function as flexible menus of best practices, warning against overly prescriptive approaches that could limit innovation.

the guidelines should be presented as a menu of best practices and examples, allowing platforms to choose solutions that fit their unique services.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Proposes that guideline reviews occur at least every two years, or sooner as warranted by technological or risk environment changes in gaming and virtual platforms.

Given the pace of technological developments in gaming and virtual environments, we suggest specifying that the Guidelines be reviewed at least every 2 years, with an option for earlier review in light of emerging risks.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Stipulates a two-year review period for the guidelines, with flexibility for earlier review when dictated by developments.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Emphasizes the need for improved access to robust, regularly updated data as essential for evidence-based policymaking and monitoring of child online safety interventions.

improved access to data is vital to develop evidence-informed policy");

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Reinforces calls for guideline review at a minimum every two years to keep pace with technology in gaming and virtual environments.

Given the pace of technological developments in gaming and virtual environments, we suggest specifying that the Guidelines be reviewed at least every 2 years, with an option for earlier review in light of emerging risks.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Proposes regular collection of user feedback, particularly from children, and public reporting of implemented improvements to support adaptive, evolving protections.

Platforms should regularly solicit feedback from child users on how well the support tools meet their needs, and publicly report improvements.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recommends a clear two-year review cycle, advocates for indicators to interpret 'best interests of the child,' and encourages dynamic updates based on developments.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

Børns Vilkårs Comments on the Commission’s Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Welcomes openness to future measures beyond those explicitly described, supporting adaptability in response to evolving risks for children online.

We welcome that the guidelines explicitly state that the measures described are not exhaustive and that additional or future measures may be identified to help online services providers meet their obligations under Article 28(1) of the DSA.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Requests inclusion of precise, practical best-practice examples in DSA guidance to improve clarity and legal certainty for all involved.

Ergänzungsvorschlag BMASGPK: In den Leitlinien sollten daher präzise, aussagekräftige Beispiele aus der Praxis angeführt werden, die als „Best Practices“ gelten und welche auch zu mehr Rechtssicherheit für alle Beteiligten führen könnten.

Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology). Stresses the importance of including independent scientific research in platform assessments and policy measures related to minors’ online safety.

The guidelines should emphasise the necessity of taking into account independent scientific research regarding the assessment of whether platforms should be considered 'accessible to minors', the effectiveness of age assurance methods, the assessment of risks and the effectiveness of other measures, such as transparency of ad disclosures.

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 (European Commission). Sets out that guidelines will be reviewed as needed according to practical experience and societal, technological, or regulatory developments, with possible amendments after consultation.

The Commission will review these guidelines as soon as this is necessary in view of practical experience gained in the application of that provision and the pace of technological, societal, and regulatory developments in this area.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Underlines the importance of timely reviews of DSA-related guidelines as the landscape rapidly evolves.

The general evaluation of the DSA can also lead to updates, which will need to be re- flected in the guideline

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Calls for clearer guidance on balancing children's rights and determining appropriate levels of privacy, safety, and risk in digital services.

The Commission should provide guidance on how providers should balance children's rights to avoid disproportionate measures that may risk children's fundamental rights.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Advocates for periodic information sharing and updates to the guidelines to keep pace with fast-evolving technologies and user behaviors.

la forte évolution des techniques et des usages appelle à organiser une remontée et un partage d'informations périodiques, en particulier afin de réactualiser les lignes directrices le cas échéant.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Requests additional Commission guidance and tools for effective and harmonized child rights impact assessments, with interim reliance on recognized best practices.

Furthermore, further guidance on the tools to be used to carry out child rights impact assessments is needed to ensure effectiveness and harmonization.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Recognizes and supports the integration of state-of-the-art research and expert evidence as the basis for guideline development for minors’ safety online.

The draft guidelines incorporate important evidence from a range of expert external sources, including academics, civil society organizations, regulators in other jurisdictions, and international governance bodies.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Emphasizes that guidelines for minors' online safety should be regularly reviewed due to the fast-changing digital environment.

Due to rapid developments in this field, a static set of recommendations is not sufficient.

Contribution from medical professionals regarding the Draft Commission Guidelines on the Protection of Minors Online (Article 28 DSA) (Youth Smoking Prevention Foundation (Stichting Rookpreventie Jeugd); #vapenjouwkeuze). Supports calls for the Commission to provide explicit, concrete guidance based on high international standards, notably the UNCRC General comment No. 25.

38 leading children's rights organizations and experts urge the Commission to provide "clear and concrete guidance based on UNCRC General comment No. 25 and the highest available standards".

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Seeks greater clarity regarding what additional risk mitigation measures might be expected under DSA articles beyond the guidelines as written.

it remains unclear what "additional measures" (line 97) may be expected of VLOPs in practice.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Promotes a focus on continuous improvement and effective public reporting for governance, rather than compliance checklists and duplication of effort.

We further encourage the Commission to clarify that public reporting and documentation of governance structures should be focused on demonstrating good-faith compliance and continuous improvement, not on meeting rigid procedural checklists.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Endorses clear and regular review mechanisms (e.g., biennial reviews) for the guidelines, as well as added support tools for risk reviews and more precise definition of the child's best interests.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). Seeks more specific guidance on how frequently platforms should review and update their risk status, reflecting the dynamic nature of online environments.

The section on risk assessment also raises the question of how often the risk status is to be reviewed and renewed by a platform.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Supports timely publication of EU Commission guidance and tools to assist providers in conducting robust risk assessments as part of ongoing improvement efforts.

Aus diesem Grund regt sie an, dass die Europäische Kommission zeitnah die angekündigten Orientierungshilfen und Werkzeuge veröffentlicht, um die Anbieter bei der Durchführung der Überprüfung zu unterstützen.

1.4.11 Miscellaneous

This category emphasizes the importance of avoiding overly simplistic or deterministic approaches in regulating emerging technologies, particularly in the context of risk assessment, transparency, and oversight. The key insight is a caution against embracing 'techno-determinism' (the belief that technology alone determines social outcomes) and 'techno-solutionism' (the idea that technology can provide quick fixes to complex societal issues). Instead, it suggests that thoughtful, multifaceted oversight is necessary for effective regulation, especially for sensitive concerns such as child safety online. Key quotes in this category underscore the historical failures of relying solely on technology to solve complex societal challenges, highlighting the need for comprehensive strategies beyond technical interventions.

> *As the history of technology repeatedly shows us, techno- deterministic and techno-solutionist approaches are unlikely to achieve their purported goals").* (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

1.5 Content Moderation and Harm Prevention

The most compelling insight across content moderation and harm prevention is the call for adaptable, evidence-based measures that proactively protect minors from a wide spectrum of harms, while actively involving children, experts, and diverse stakeholders in shaping definitions and policies. Sub-categories converge on the importance of expanding harm definitions beyond explicit risks to encompass cumulative, often subtle dangers—such as discriminatory rhetoric, manipulative design, and evolving technological threats like AI-generated content—so that policy keeps pace with digital realities. Transparent and enforceable moderation standards, anchored in regulatory frameworks like the DSA, are emphasized alongside the necessity for accessible reporting tools, age-appropriate user support, and clear communication of outcomes to minors. Automation and AI offer powerful safeguards but must be balanced by human oversight and culturally sensitive, locally adapted practices; "measures that reflect local language nuances and lived realities" are repeatedly highlighted as essential for effectiveness. Robust technical solutions must tread carefully to avoid over-blocking or disproportionately suppressing lawful expression, with labelling, credible flagging, and multi-layered review systems cited as important tools. There is a common recognition that children's rights, autonomy, and wellbeing—especially for those from vulnerable or marginalized groups—must be central. Across all sub-categories, the trend is toward collaborative, flexible, and proportionate moderation ecosystems that balance protection with freedom of expression, tailored for rapidly changing risk landscapes and the diverse needs of young users.

1.5.1 Harmful Content Definition and Scope

The category 'Harmful Content Definition and Scope' encompasses a strong consensus that definitions of harmful content, particularly as they relate to children and minors online, must be expanded significantly beyond the traditional focus on pornography and gambling. Contributors call for guidelines that encompass a broader range of risks, including violence, self-harm, disordered eating, discriminatory behavior (e.g., misogyny or anti-LGBTQI rhetoric), and the cumulative impact of exposure to even non-explicit but potentially damaging material. The need for clarity, transparency, and stakeholder involvement—especially with civil society, children, and independent experts—is consistently emphasized for developing these definitions. There is also recognition of the dangers of vague or overly broad definitions, which could lead to unjustified censorship, legal uncertainty, and the suppression of lawful content. Several insights warn against applying physical-world analogies to online content moderation or imposing subjective standards that could disproportionately impact marginalized communities. The importance of clear, evidence-based, and regularly reviewed classifications is echoed throughout the documents. Finally, some submissions call for the explicit inclusion of new risk factors such as online addiction and emerging technologies (e.g., AI-generated content), ensuring that policy keeps pace with digital developments.

> *Include the full overview of described harms that VLOPs are having on children, going well beyond what pornography and gambling.* (Ten recommendations to the European Commission to really protect children online (unknown))

> *Overall, the guidelines fail to provide a clear definition of what constitutes "harmful" or "illegal" content, leaving room for discretionary overreach and unjustified content removal.* (Securing a high level of privacy, safety and security for minors online (SUPERRR Lab))

> *Define clearly and transparently what the platform considers as content and behaviour that is harmful for minors' privacy, safety and security, ideally in cooperation with independent experts and civil society.* (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 (European Commission))

> *In a polarized social context where the definition of 'harmful' is highly subjective and deeply influenced by politics, allowing the government to decide which content is considered 'harmful' opens up a serious vector for abuse");* (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

> *Online platforms must not only consider risks to individual children but also systemic risks such as normalization of surveillance, commercial pressure, and mental health deterioration.* (Ten recommendations to the European Commission to really protect children online (unknown))

Implementation: Clear categorical definitions with examples (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Urges the expansion of the understanding of harms to children online by including a broader set of risks, such as content promoting violence and discrimination, not just pornography and gambling.

Other forms of harmful content, including content promoting violence, self-harm, disordered eating, or discriminatory behaviour (e.g., misogyny or anti-LGBTQI rhetoric), are well-documented mental health risks to minors and need to be included.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates for collaboratively defining and classifying harmful content for minors, including input from children and independent experts, and ensuring these definitions are regularly reviewed.

Define and classify clearly and transparently what the platform considers as content that is harmful for minors' privacy, safety and security when encountered repeatedly, in cooperation with independent experts, civil society and children themselves.

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Calls for the explicit inclusion and regulation of soft-core pornography and sexualized influencer content as age-inappropriate, which are often not covered by current frameworks.

The current framework should be expanded to explicitly capture soft-core pornography and sexually suggestive content-including influencer media, stylized nudity, fetishized trends, and other borderline content-which may evade illegality but clearly undermine the well-being of minors.

Ten recommendations to the European Commission to really protect children online (unknown). Emphasizes the necessity for guidelines to address a comprehensive spectrum of harms to children, going beyond the conventional focus areas.

Other forms of harmful content, including content promoting violence, self-harm, disordered eating, or discriminatory behaviour (e.g., misogyny or anti-LGBTQI rhetoric), are well-documented mental health risks to minors and need to be included.

Salminen contribution protection of minors (Aalto University). Highlights the diverse approaches platforms adopt regarding content featuring children and the balance between freedom of expression and the safety and protection of minors.

While the issue intersects with fundamental rights–particularly the right to freedom of expression–they also raise serious questions of safety and child protection.

CONCLUSION & POLICY DEMANDS (unknown). Recommends a comprehensive overview of online harms to minors, advocating for guidelines that go well beyond just pornography and gambling.

Other forms of harmful content, including content promoting violence, self-harm, disordered eating, or discriminatory behaviour (e.g., misogyny or anti-LGBTQI rhetoric), are well-documented risks to minors and need to be included.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Expresses concern about requiring global platform providers to label content as 'harmful' based on varying definitions of illegality across jurisdictions, warning of legal conflicts.

even national laws of Member states have different thresholds for illegality.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Stresses the need to expand the definition of harmful content and provide clear categories and examples to aid implementation.

Current limitation: Guidelines focus on pornography and gambling

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Advocates for the use of clear, categorical definitions and examples in defining harmful content.

Implementation: Clear categorical definitions with examples

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Notes the limitation of current guidelines to pornography and gambling, and reiterates the need for broader categorical clarity.

Current limitation: Guidelines focus on pornography and gambling

EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform). Suggests augmenting the CSAM Regulation to recognize pornography as an exacerbating factor in child sexual abuse cases.

Enrich the CSAM Regulation including pornography as an exacerbating factor of child sexual abuse

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Warns that subjective definitions of harm can lead to government overreach, suppression of lawful information, and particularly affect marginalized youth.

segregate-and-suppress laws can effectuate "a digital erasure of access to information for and about LGBTQIA+ youth");

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Criticizes vague definitions of 'harmful' content in guidelines, stating this can result in legal uncertainty and potential over-censorship, especially via automation.

Overall, the guidelines fail to provide a clear definition of what constitutes "harmful" or "illegal" content, leaving room for discretionary overreach and unjustified content removal.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Notes the challenge of achieving clear definitions of harmful content across cultures, and the risks of leaving content decisions to algorithms without explicit criteria.

Considering a clear and finite definition of harmful content may not always be achieved due to conflict of interests or the bridging of cultural gaps, platform providers need to be absolutely clear on what constitutes harmful behaviour as they may, otherwise, run the risk of an algorithm making an ultimate decision as to whether to display specific content, which may lead to further issues.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Calls for clear, categorical definitions with examples when expanding the scope of harmful content.

Implementation: Clear categorical definitions with examples

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Advocates for a clear, evidence-based definition of online addiction to be included in guidelines, citing the need for clarity for prevention and intervention.

Die Leitlinien sollten eine klare, evidenzbasierte Definition von Online-Sucht bzw. „suchtähnlichem Nutzungsverhalten“ enthalten - entsprechend der WHO- Klassifikation „Gaming Disorder“ in ICD-11.

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 (European Commission). Stresses the importance of clearly and transparently defining what constitutes harmful content and behaviors for minors, ideally in consultation with stakeholders.

Define clearly and transparently what the platform considers as content and behaviour that is harmful for minors' privacy, safety and security, ideally in cooperation with independent experts and civil society.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Suggests providing clear definitions and practical categories of inappropriate content for minors to aid platforms in risk identification and mitigation.

This entails outlining clear and practical definitions of what constitutes inappropriate content for minors and how the particular type of content should be categorized based on its harmful nature, in order to help the individual industries to iden- tify and mitigate risks.

Feedback for 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 (xHamster). Highlights the lack of specific definitions for 'age-inappropriate content' in current guidelines and emphasizes its necessity.

The Guidelines make references to "age inappropriate content". However, there is no specific clarification of what this specifically contains.

Ten recommendations to the European Commission to really protect children online (unknown). Stresses the need for guidelines to address all forms of harm to minors, far beyond the usual suspect categories.

Other forms of harmful content, including content promoting violence, self-harm, disordered eating, or discriminatory behaviour (e.g., misogyny or anti-LGBTQI rhetoric), are well-documented mental health risks to minors and need to be included.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Points out the risk posed by cumulative exposure to content, even if not individually harmful, and suggests this should be addressed in harm definitions.

We consider it critical to consider the harm produced by the cumulative impact of seeing what may be considered as non-harmful content (lines 551-556).

Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation). Advocates for a stronger, zero-tolerance position on harmful content, clearly defining both illegal and legal but age-inappropriate or abusive material.

Harmful content should cover illegal material (such as child sexual abuse material, hate speech, or incitement to violence), but also legal but harmful content that may be age-inappropriate, sexually explicit, violent, including content that normalise or encourage discriminatory attitudes, biases, radicalisation or abusive behaviour as well as promoting self-harm.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Calls for clear distinctions between illegal and harmful content in Digital Services Act implementation, to avoid confusion and ensure effective moderation.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Recommends explicit provider commitments against violence towards children online and suggests clearer regulation of new risks like AI-generated content.

Es wird empfohlen, in den Leitlinien die Anbieter dazu zu ermutigen sich ein Leitbild zu geben, im Rahmen dessen sich diese sichtbar gegen Gewalt an Kindern und Jugendlichen positionieren unter expliziter Nennung der Gewaltformen wie bspw. Grooming oder die Verbreitung von Missbrauchsdarstellungen.

1.5.2 Transparency and Regulatory Compliance

The category 'Transparency and Regulatory Compliance' under content moderation and harm prevention highlights the necessity for clear, enforceable, and transparent standards in platform governance, especially for

the protection of children online, in alignment with regulatory frameworks such as the EU Digital Services Act (DSA). Key knowledge embedded in these insights includes the importance of industry-wide protocols for content warnings, systematic identity and content verification, and transparent moderation standards, preferably developed with expert collaboration. Several contributions underscore the need for detailed transparency reporting, robust labelling of AI-generated content, and minimum standards for moderation—such as defined response times and clear user reporting mechanisms. A recurring emphasis is placed on ensuring that regulatory measures do not inadvertently lead to overreach or suppression of legitimate speech, with calls for proportionate, objective enforcement and clear distinction between harmful and illegal content. Practical implementation tools, like Terms and Conditions, must be aligned with legal requirements and used judiciously. Stakeholders propose that transparency extends beyond policies to include user-friendly disclosures, reporting menu systems adapted for minors, and mechanisms for users to report or understand moderation decisions. A notable concern is the risk of misuse of regulatory frameworks for censorship, and the challenge of ensuring that new technologies like AI are properly labelled and managed to prevent manipulative or deceptive use. Effective transparency and regulatory compliance thus require a combination of technical measures, policy clarity, enforceable timelines, and safeguards against misuse—all ideally developed collaboratively and made accessible to the broadest range of users, including children.

> *We would also like to expressly emphasize that the clear and transparent definition of moderation standards should ideally be developed in collaboration with experts.* (Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)))
>
> *14 DSA, online platforms must: 81.1. include information on any restrictions that they impose in relation to the use of their service in respect of information provided by users in their terms and conditions; and 81.2. act in a diligent, objective and proportionate manner in applying and enforcing these restric* (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))
>
> *We recommend that the guidelines provide a defined minimum standard for platforms moderation policies and procedures, which includes a set period of time to act upon content that is detected as harmful for the privacy, safety and security of minors, as well as mandated transparency on how the platform manages reports and complaints of content on their platform.* (Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group))
>
> *A complete end-to-end identity verification and content moderation solution to prevent uploaders from publishing illegal content on user-generated content platforms, ensuring a safe, trustworthy, and compliant online experience for everyone.* (Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy))
>
> *The recommendations should include specific measures for detecting and flagging AI-generated videos and audio, especially those that may appear misleading or manipulative.* (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))
>
> *Establishing clear requirements for users to disclose when content, including but not limited to videos and audio, has been generated or significantly altered by artificial intelligence.* (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Proposes the establishment of industry-wide warning label protocols for harmful content to enhance transparency and protection across platforms, not just through contextual warnings.

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). Advocates for robust identity verification and content moderation on user-generated content platforms to ensure compliance with the Digital Services Act and prevent illegal uploads.

A complete end-to-end identity verification and content moderation solution to prevent uploaders from publishing illegal content on user-generated content platforms, ensuring a safe, trustworthy, and compliant online experience for everyone.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Warns against the potential for regulatory frameworks to be misused for censorship, emphasizing the need for transparency and protection of legitimate speech.

Tools meant to nudge users or demote harmful content can easily slip into soft censorship, where platforms or governments suppress legitimate speech under the guise of harm reduction.

DOT Europe response1 (DOT Europe). Requests clarification that content moderation obligations under Article 28 of the DSA should apply only to platforms within its defined scope, preventing regulatory overreach.

we flag that subsequent paragraphs, namely I. 709 to 713, could be interpreted as going beyond the initial scope of Article 28, which is directed at services qualifying as online platforms.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Highlights the need for clear, transparent, and child-friendly moderation standards, ideally developed with expert input, as an extension of DSA Article 28(1).

We would also like to expressly emphasize that the clear and transparent definition of moderation standards should ideally be developed in collaboration with experts.

Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act Allwyn submission (Allwyn). Supports the 'note and take down' approach to illegal content under the DSA and encourages operator cooperation with authorities to ensure compliance and legal communications.

Beyond underage prevention, we support the DSA 'note and take down' approach to illegal content and cooperate with national authorities to signal commercial communications on non- licensed gambling services.

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Suggests that Terms and Conditions should only be used to moderate content that is legal but potentially harmful to minors, and not as a substitute for legal provisions.

In other words, Terms and Conditions can only be used, where applicable, as an implementation tool for Article 28 in cases where the content is legal for minors but may, under certain circumstances, be potentially harmful to them.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Calls for a bold, technically sound, and enforceable implementation of Article 28(1), recognizing the opportunity to set new standards in protecting minors online.

We urge the Commission to adopt a bold, technically grounded, and enforceable approach to implementing Article 28(1), drawing on Thorn's extensive experience in developing technical interventions and collaborating directly with technology companies and enforcement bodies.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Stresses that online platforms must transparently communicate any user information restrictions in their terms and conditions, and enforce these objectively and proportionately.

14 DSA, online platforms must: 81.1. include information on any restrictions that they impose in relation to the use of their service in respect of information provided by users in their terms and

conditions; and 81.2. act in a diligent, objective and proportionate manner in applying and enforcing these restric

Feedback for 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 (xHamster). Recommends that transparency reporting obligations be reflected in both reporting categories and user menu structures, and that these be adapted to be understandable, especially for minors.

At the same time, Guidelines contain this statement: "If reporting categories are used, ensure that they are adapted to the youngest users allowed on the platform. Complex menu systems should be avoided. There should also be an option available that allows minors to provide their own reasons for a report."

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Advocates for explicit labelling and moderation of AI-generated content, with strong detection mechanisms and prohibition of unlabeled AI uploads to ensure user clarity and safety.

Moreover, the uploading of AI-generated content without clear labelling as such should be expressly prohibited and subject to effective moderation.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Recommends defining clear minimum standards for moderation policies, including prompt action on harmful content and transparency regarding complaint handling.

We recommend that the guidelines provide a defined minimum standard for platforms moderation policies and procedures, which includes a set period of time to act upon content that is detected as harmful for the privacy, safety and security of minors, as well as mandated transparency on how the platform manages reports and complaints of content on their platform.

1.5.3 Content Moderation Processes and Enforcement

Content moderation processes and enforcement under the DSA, especially regarding the protection of minors, is a multifaceted domain integrating proactive moderation measures, human oversight, and context-sensitive enforcement. Many contributions emphasize the importance of both automated and human review systems, particularly for user-generated, high-reach, or risky content. There is a strong call for platforms to develop clear and enforceable moderation policies, with some stakeholders arguing for mandatory minimum standards while others highlight the need for flexibility based on risk, product category, and practical operational limits. Trusted flaggers, real-time feedback mechanisms, and the combination of AI and human judgment are cited as effective elements in contemporary moderation ecosystems. A substantial focus is placed on the need for timely removal of illegal or harmful content (especially sexual and predatory material targeting minors), safeguards around AI and synthetic content, and careful differentiation between content types (e.g., lotteries versus riskier gambling products). Human moderation is seen as both a safeguard against moderation failures and a requirement in cases of widespread or potentially viral content. Some actors also highlight the need for support and supervision for moderation teams due to the emotionally demanding nature of their work. Overall, the insights reflect a balance between strong enforcement, the recognition of legacy moderation practices, tailored approaches for different sectors, and the need for both technical and human resources.

Establish moderation policies and procedures that set out how content and behaviour that is harmful for the privacy, safety and security of minors is detected and how it will be moderated and ensure that these policies and/or procedures are enforced in practice. (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 (European Commission))

Providers must implement clear and effective moderation procedures, taking into account the level of risk, the number of minors exposed, and the severity of potential harm. (Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018))

we welcome that the guidelines recognise the need for human review for viral content and accounts that may pose a risk of harm to minors. (Public consultation on 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 (Coimisiún na Meán))

However, research shows that this such options are still provided by some platforms (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Content moderation decisions must be informed by independent scientific expertise, not only internal platform assessments. (Feedback DSA (unknown))

Guidelines should establish a deadline for removal of content that is harmful for children's privacy, safety and security. (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))

BDZV MVFP Reply to EC Art 28 DSA Draft Guidelines (BDZV Bundesverband Digitalpublisher und Zeitungsverleger e. V.; MVFP Medienverband der freien Presse e. V.). Argues that established editorial content moderation practices already satisfy DSA requirements, referencing prior legal obligations for rapid removal or blocking of unlawful content.

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Calls for stricter and better-enforced content moderation to combat non-consensual and AI-generated sexual content, prioritizing the protection of minors' privacy and safety.

Implementing technical solutions to prevent AI systems on their platform from allowing users to access or disseminate content that is harmful for the privacy, safety and/or security of minors, including any AI-generated sexual content involving minors or AI-generated intimate content depicting identifiable individuals created without consent.

Public consultation on 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 (Coimisiún na Meán). Advocates enhanced content moderation for minors, including human review for viral content, detection of synthetic media risks, and AI guardrails against harmful prompts.

we welcome that the guidelines recognise the need for human review for viral content and accounts that may pose a risk of harm to minors.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Emphasizes strengthened moderation procedures for child protection, prompt response to flagged content, and preventing circumvention of content warnings or blocks.

vidence5 shows that the measures put in place by online platforms to reduce the risk of harmful or illegal content exposure are often insufficient and content moderation failures persist.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Suggests the use of real-time feedback and warnings to reduce toxicity and empower users to edit or reconsider posting offensive material.

study of 50,000 users showed how real-time feedback reduces toxicity.

Comments on the European Commission draft 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 ("DSA") (BDZV, MVFP). Reiterates that editorial platforms' existing moderation measures, predating the DSA, remain effective and compliant with legal requirements.

We further note that editorial online platforms' implementation of effective content moderation measures predates the DSA.

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Highlights children's vulnerability to digital bullying and the need for stronger moderation tools to prevent unwanted social media contacts.

There are just so many unpleasant people who write to you . And Instagram doesn't have any filters . You can just write to everyone , even if they don't want it . "

Additional contribution (Collective Shout). Recommends algorithms, with human oversight, to rapidly identify and remove sexualized or predatory comments targeting minors on digital platforms.

Algorithms, overseen by human moderators, should be included to proactively remove sexualising or sexually graphic comments on minors' images and posts.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Recommends stronger moderation, such as screenshot blockers and blurring tools, to shield minors from harmful or misused image and video content.

vzbv supports stronger moderation measures, such as screenshot blockers and automatic blurring of explicit material.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Advocates establishing clear definitions for what constitutes problematic and repeated content per the DSA's requirements.

Additionally, it is necessary to provide clear criteria for when content is considered to be repeated in a problematic manner.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Calls for reinforced, tailored moderation tools for gaming environments, combining human and AI oversight to tackle grooming and real-time risks.

We recommend strengthening expectations around moderation tools tailored to in-game interactions, and the role of moderators as well as carefully supervised AI systems in preventing grooming, harassment, hate speech and other risks in real time.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Proposes mandatory, clearly articulated moderation procedures for platforms, with risk-based approaches and focus on effective human intervention.

Providers must implement clear and effective moderation procedures, taking into account the level of risk, the number of minors exposed, and the severity of potential harm.

The European Lotteries' Response to Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act (The European Lotteries). Argues for differentiated moderation strategies for lottery versus higher-risk gambling, ensuring proportionate content restrictions to preserve public benefit.

This differentiation should be reflected in how content is assessed and moderated on online platforms.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Recommends strengthened, supervised moderation systems—both human and AI—for in-game interactions to prevent real-time harms to minors.

We recommend strengthening expectations around moderation tools tailored to in-game interactions, and the role of moderators as well as carefully supervised AI systems in preventing grooming, harassment, hate speech and other risks in real time.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Asserts that content recommendation rules shouldn't impede platforms' ability to moderate harmful or objectionable material from user feeds.

Significantly, neither of these laws limits the platforms' ability to moderate harmful content from a feed.

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Suggests using less intrusive measures like trusted flaggers for potentially harmful content and stresses prompt removal of illegal material.

In particular, for content that may be classified as "potentially harmful," trusted flaggers can play an important role.

Feedback DSA (unknown). Urges moderation based on independent scientific expertise, thorough coverage beyond high-traffic spaces, and nuanced content-level approaches for sensitive or radicalized communities.

Don’t restrict human moderation only to high-traffic content.

Microsoft response to the European Commission's draft 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 (Microsoft). Warns of the practical limitations of universal human review and recommends moderation processes be adaptable to harm type and scale.

we note that the draft Guidelines recommend prioritizing moderation and human review in certain circumstances, which may not be practical in the context of an all-up content moderation process for an online platform.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Supports strong ongoing moderation for minors' safety; urges caution regarding automatic restriction of unverified flagged content and emphasizes action based on terms and relevant law.

Our ongoing enforcement of Community Guidelines against illegal and harmful content, including scams, child safety issues, and harassment, directly supports the Guidelines' call for strong moderation practices to ensure minors' privacy, safety, and security.

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 (European Commission). Drafts specific policies for detecting, moderating, and prioritizing harmful content for minors, considering risk, impact, and audience size, and recommends human review in high-risk cases.

Establish moderation policies and procedures that set out how content and behaviour that is harmful for the privacy, safety and security of minors is detected and how it will be moderated and ensure that these policies and/or procedures are enforced in practice.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Recommends instituting human review for content that greatly surpasses certain impact or reach thresholds.

Put in place human review for content that substantially exceeds

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Supports the centrality of moderation and trusted flaggers in reducing minors’ exposure to harm, especially where content crosses platform boundaries.

We support the guidelines' focus on the importance of moderation to reduce minors' exposure to harmful content behaviour.

Input from the ECA to the Guidelines on protection of minors online under the Digital Services Act (European Casino Association (ECA)). Advocates recognition of legitimate industry groups and gambling authorities as trusted flaggers to enhance accuracy and speed in moderating gambling-related content.

Granting trusted flagger status to recognised European industry associations like the ECA and national gambling regulatory authorities would empower platforms to act more swiftly and accurately when moderating gambling-related content.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Details Epic Games' practice of moderating user-generated content by combining algorithmic and human review prior to public access, focusing on legality and policy adherence.

All Fortnite Islands are moderated using a combination of automated and human review, before they are published and made available to players.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Recommends clear, specific requirements for human review of widely viewed content and mandatory deadlines for removing harmful material affecting minors.

We suggest a change in the wording in line 699: rather than "consider" human review, "ensure" human review.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Encourages platforms to provide both individual and team supervision for moderation and complaint teams, recognizing the emotional impact of exposure to disturbing content.

Aufgrund der expliziten Inhalte, denen insbesondere Beschwerdeteams und Moderatorinnen ausgesetzt sind, sollten Team- und Einzelsupervisionen als Fürsorgemaßnahmen der Anbieter in den Leitlinien Erwähnung finden.

1.5.4 User Reporting, Appeals, and Support

The category of User Reporting, Appeals, and Support in the context of content moderation for minors reflects a range of key insights encompassing the accessibility, effectiveness, and safety of reporting and complaint mechanisms for young users. Across the documents, there is strong emphasis on designing age-appropriate, intuitive, and easily accessible reporting tools—often recommending that support options be available within a couple of clicks and integrated with national helplines or support services when minors are at risk. Many contributions highlight the need for transparency, child-friendly interfaces, standardization of reporting buttons, and clear explanations to minors about the outcomes and handling of their reports. There is also notable focus on preventing misuse of reporting options, such as arbitrary or retaliatory reports, and ensuring that these systems do not unduly limit minors' access to information based on subjective judgments. Various stakeholders advocate for the prioritization of reports based on risk and severity rather than the age of the reporter, and for clear response timelines and escalation paths for urgent issues. There is frequent attention to the role of trusted flaggers, independent appeals, and the necessity for human oversight with cultural and linguistic expertise. Finally, stakeholders underscore the importance of protecting minors from retaliation and ensuring follow-up support, while cautioning about the resource limitations of smaller platforms and the risk of making helplines an extension of platform support rather than independent aids.

These tools must enable children to easily report inappropriate content or behaviours, using language they can understand and ensuring a prompt response, with prioritisation of reports submitted by minors. (Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018))

Effective and child-friendly user reporting, feedback and complaint tools enable minors to express and address features of online platforms that may negatively affect the level of their privacy, safety and security. (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 (European Commission))

the guidelines should also recommend to ensure there is a link between reporting tools and support services, to facilitate access to safety for children who are at risk of in a situation of harm. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

We are pleased to see that the Commission has addressed the need for minors to be informed about who their reports are shared with (line 777). This is a crucial step in preventing and addressing risk and harms occurring through the platforms. (UNICEF Sweden's comments on the protection of minors guidelines under the Digital Services Act (UNICEF Sweden))

Instead, services should maintain the discretion to utilise user feedback in a way that appropriately balances user rights with the mitigation of risks to minors. (Response to the consultation on the

European Commission's draft 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 (LinkedIn Ireland Unlimited Company))

orn commends the inclusion of child-friendly reporting tools and recommends expanding these provisions by: · Embed real-time reporting features into platform UI, including clear escalation mechanisms for grooming and abuse. (Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Emphasizes the need for reporting mechanisms for age-inappropriate content to rely on objective criteria to avoid misuse and excessive restriction of minors' information access.

This approach carries a high risk of misuse and could unduly restrict minors' access to information based solely on the subjective views and sensitivities of others.

Contribution Guidelines art 28 DSA (Respect Zone). Recommends visible and accessible reporting features for minors, including mandatory human assistance and strengthened roles for trusted flaggers on youth-accessible platforms.

Platforms accessible to minors should integrate a visible and accessible reporting feature within their chatbots or conversational agents, allowing users to: · be redirected to the appropriate reporting form, · be informed of their rights (especially for minors), · access human assistance or support if

UNICEF Sweden's comments on the protection of minors guidelines under the Digital Services Act (UNICEF Sweden). Highlights minors' reluctance to report harmful behavior due to fear of retaliation and calls for complaint mechanisms that protect them from negative consequences.

Based on our consultations with children about their digital environments, it is clear that many hesitate to report unwanted or inappropriate behaviour on online platforms because they fear that the person they report will be notified - and they worry about possible consequences.

OFFLIMITS (Stichting Offlimits). Stresses the importance of giving priority to reports from DSA-designated Trusted Flaggers like Offlimits, ensuring swift processing of their submissions.

This designation further enhances the established trusted relationships with major online platforms, ensuring that reports submitted by Offlimits regarding illegal content are treated with priority and without undue delay.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates for child-friendly, accessible reporting linked to support services and revisiting reporting tools to address issues such as adults posing as minors.

the guidelines should also recommend to ensure there is a link between reporting tools and support services, to facilitate access to safety for children who are at risk of in a situation of harm.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Calls for large platforms to implement independent appeal mechanisms, including culturally and linguistically competent human reviewers for content decisions.

Amnesty International recommends adding that large social media platforms should provide mechanisms for independent appeal of decisions to restrict - or not restrict - content that should include independent human review by persons with knowledge of the linguistic and cultural context relevant to the decision in addition to the minimum requirements defined by the Digital Services Act, including the right to substantiate a complaint with evidence and to a reasoned decision.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Supports the establishment of transparent, user-friendly complaint and reporting mechanisms that inform users about the outcomes of their reports.

establishing and operating transparent and user-friendly mechanisms for users of a video-sharing platform to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 provided on its platform;

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Warns of the limitations of using reporting categories for minors and stresses clarifying follow-up actions post-reporting.

Bris understands the need for categorization but wishes to emphasize that this is something that may limit children's ability to report.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Recommends setting explicit and maximum response times for platforms handling minors' reports of illegal or harmful content.

Insert explicit maximum response times by online platforms in the event that a minor reports illegal/harmful content.

DOT Europe response1 (DOT Europe). Argues against prioritizing reports from minors by default, insisting that only Trusted Flaggers be given automatic priority per DSA.

As per the DSA text, only entities awarded the status of Trusted Flaggers can see their notices treated with priority.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Emphasizes accessible (two-click) reporting and immediate review in cases presenting serious risks to minors.

Reporting systems are essential for ensuring user safety, maintaining content quality, and upholding legal and community standards. It empowers users to flag harmful, abu- sive, or misleading content, enabling online platforms to take timely action and enforce guidelines effectivel

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Recommends setting reasonable response times and prioritizing complaints according to the harm risk, not just the identity of the reporter.

These should be prioritised according to the risk of harm and the other factors mentioned earlier in the guidelines.

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 (BeSmartOnline! Maltese Safer Internet Centre). Endorses intuitive, accessible, and age-appropriate reporting tools for minors on platforms.

We strongly endorse the emphasis on accessible, age-appropriate reporting tools.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Supports effective, age-appropriate reporting and helpline tools, ensuring quick and understandable ways for minors to report issues.

These tools must enable children to easily report inappropriate content or behaviours, using language they can understand and ensuring a prompt response, with prioritisation of reports submitted by minors.

Child Focus Contribution to the Public Consultation on the Protection of Minors guidelines under the Digital Services Act (Child Focus). Calls for standardized reporting symbols and mechanisms and the integration of support referrals, clarifying the role of trusted flaggers.

reporting buttons should be standardised across platforms using universal symbols or icons.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Advocates for clear response timeframes, escalation for urgent reports, and prevention of arbitrary or revenge reporting by minors.

Platforms should be required to respond to children's reports within clearly defined time limits and must have protocols for rapidly escalating urgent issues such as grooming attempts or self-harm content.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Suggests complaint prioritization be based on impact to minors' safety, not solely who submits the report.

Adult users might report or complain as well to protect minors.

Microsoft response to the European Commission's draft 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 (Microsoft). Cautions against unqualified content feedback mechanisms for minors and highlights the risk of misuse if too broadly implemented.

Equally, the proposed mechanism for minors to provide feedback on content that they don't want to see should also have some qualifications for its application: this seems best suited only to those platforms where minors are being recommended user generated content and could be refined to reduce risk of misuse or disproportionate use.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Recommends real-time reporting and escalation features for grooming and abuse, embedded within platform interfaces for minors.

orn commends the inclusion of child-friendly reporting tools and recommends expanding these provisions by: · Embed real-time reporting features into platform UI, including clear escalation mechanisms for grooming and abuse.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Argues against giving minors additional reporting/appeal rights beyond what the DSA grants all users, and for prioritizing based on content type.

It is unclear why the Guidelines propose that minors receive additional due process rights compared to the already extensive due process rights the DSA provides to all users

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Suggests a unified, easily locatable child-friendly reporting contact point and clear education about trusted flaggers for minors.

Weiters wäre es sinnvoll, einen für Kinder leicht auffindbaren und verständlichen Hinweis auf die Trusted Flagger und deren Aufgabe zur Verfügung zu stellen.

Guidelines to ensure high levels of privacy, safety, and security for minors online (Kaspersky). Supports child-empowering mechanisms for reporting content or behaviors that may violate terms, strengthening minors' control.

we support the Commission's proposal to implement mechanisms that enable minors to report content, activities, individuals, accounts, or groups they believe may violate a platform's terms and conditions.

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 (European Commission). Outlines baseline requirements for effective, accessible and child-friendly reporting, feedback, and support tools for minors.

Effective and child-friendly user reporting, feedback and complaint tools enable minors to express and address features of online platforms that may negatively affect the level of their privacy, safety and security.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Notes challenges faced by minors in finding and using reporting tools, despite their importance.

n Denmark, the experience is that minors seldomly utilise the option of reporting ille- gal content to the online platforms, as they either are not aware that this option exists or as they find it difficult to report the content in practice.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Insists on prompt responses to reports from minors about illicit content, along with feedback regarding action taken.

En cas de signalement par un mineur d'un contenu illicite ou d'un comportement déplacé par un autre utilisateur, la plateforme devra agir promptement et informer le jeune des démarches entreprises pour le traiter.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Calls for easily reviewable, regularly updated, and user-feedback informed reporting mechanisms, allowing minors to mark some issues as urgent.

Platforms should enable minors to provide feedback regarding the reporting mechanisms and regularly review reporting mechanisms based on this feedback to ensure their effectiveness and relevance for minors"

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Emphasizes the need for genuine child-friendly support without shifting the responsibility of support from platforms to EU helplines.

Overall, we find that the guidelines lack a focus on the providers obligation to ensure child- friendly feedback on reports issued by minors.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Details Epic's reporting mechanisms for illegal or policy-violating content, including appeal processes compliant with DSA regulations.

Article 16 of the DSA already requires that Epic provide a mechanism where users can report alleged illegal content or behavior.

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). Suggests user reports based on inappropriateness for minors should not compel removal unless the content is illegal or against platform policies.

To ensure services can act consistently and transparently in accordance with Articles 16 and 17 of the DSA, reporting of items as "inappropriate" or "undesirable" for minors should not compel services to remove or take action on items that are neither illegal nor policy violating.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Argues prioritization of reports should be risk- and severity-based, not based solely on the submitter's age, for better protection of minors.

the prioritisation of user reports under Article 28 should not rest on the identity of the person submitting the report. Instead, the determining factor should be the nature and severity of the harm described in the report, particularly where the harm poses risks to the privacy, safety, or well-being of minors.

Feedback on the draft Commission guidelines on DSA article 28 (Swedish Agency for the Media). Questions the practicality of certain recommendations and highlights the need for children to document problematic content responsibly.

Children's rights organisations recommend that children who encounter problematic content online take screenshots of said content so it can be shared with relevant organisations/authorities.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Advocates for enabling non-users to report harassment, efficient handling of fake profile reports, and referrals to support services, especially in cases of adults posing as minors.

We also believe it is important that non users can report fake profiles - and other forms of digital harassment and abuse - and that the platform handles these reports efficiently (line 771).

European Commission Article 28 Guidelines Feedback (unknown). Emphasizes effective, supportive, and easy-to-use reporting tools for minors, including immediate support upon submitting a report.

Provide immediate support and relief to the minor, independent of the evaluation process of the content or contact relative to platform policies.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). Argues against fixed response times or prioritization for minor-submitted reports due to resource limitations and unpredictable circumstances.

Lastly, we do not recommend establishing a set time limit for reports or complaints made by minors.

1.5.5 Algorithmic and Technical Safeguards

The insights in the category of Algorithmic and Technical Safeguards under Content Moderation and Harm Prevention reflect a broad consensus on the need for robust, nuanced, and transparent technical solutions to protect minors online. Key approaches include implementing advanced AI-driven moderation tools, enhanced detection algorithms (such as credibility scoring, early warning systems, and machine learning classifiers), and technical mechanisms like real-time content flagging and blocking of harmful search terms or suggestions tailored for children's safety. At the same time, many contributions emphasize the risks of over-blocking and advocate for safeguards that do not unduly limit access to legitimate or educational content, using strategies such as labelling potentially harmful but legal material and referring users to authoritative sources. Innovative suggestions spotlight the value of maintaining updated multilingual registries of emerging risky terms, leveraging behavioral data with strong safeguards, and refining automated moderation to prevent unintended consequences, like lumping legitimate content with illicit material. Platforms are encouraged to collaborate with expert organizations, integrate technical identifiers for blocking alternate accounts, and remain adaptive to evolving risks. Ultimately, the insights highlight the delicate balance between technical enforcement and upholding fundamental rights like freedom of expression and access to information for minors.

technical safeguards must be integrated-particularly within generative Al systems-to prevent access to, production of, or dissemination of harmful content. (Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018))

Put in place effective technologies, internal mechanisms and preventative features to reduce the risk of content and behaviour that are harmful to minors' privacy, safety of security from being shown to minors in their accounts' interface or other functionalities of the service, including: (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 (European Commission))

We are concerned that automated content or search filters (as proposed in line 568 ff.) will lead to over-blocking, as demonstrated by a recent example from the United States. (Securing a high level of privacy, safety and security for minors online (SUPERRR Lab))

Finally, some content may be legal but could be potentially harmful to certain user groups too (e.g., based on usage patterns and recommendations). In such cases, content should not be removed, but measures such as labelling or signaling (by trusted flaggers, for example) could be implemented. (COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation))

Rather than a categorical prohibition, providers should be permitted to use behavioural data for the specific purpose of enhancing child safety and delivering age-appropriate experiences, provided such use is clearly defined and subject to appropriate safeguards. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

The ECA on this would like to present to the European Commission a clear distinction between the risk that regulated casinos and illegal gambling operators present to EU consumers. (Input from the ECA to the Guidelines on protection of minors online under the Digital Services Act (European Casino Association (ECA)))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Advocates for detailed guidelines and adequate AI safeguards to restrict harmful or age-inappropriate outputs while avoiding excessive filtering of educational materials.

In particular, the guidelines should provide adequate safeguards to prevent AI chatbots from generating outputs that are not age-appropriate or could be harmful, such as sexual exchanges and misconduct, reinforcement of (racist) stereotypes, or advice that encourages dangerous behaviour, self-harm, or other negative impacts on a user's mental health.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Proposes algorithmic tools such as credibility scoring to counter misinformation and early-warning algorithms to minimize harmful or violent online content.

Credibility Score Algorithms boost sources rated for accuracy and transparency.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Recommends against outright blocking of harmful search terms, favoring the redirection to authoritative resources instead.

It is important to note that blocking harmful search terms outright is not always the best strategy to protect minors or users in general.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Suggests mandatory user-generated content labeling and clear information to enable more effective and targeted moderation.

Platform providers should be obliged to provide a system allowing users to indicate whether their own user-generated content is suitable only for adults.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Calls for enhanced technical safeguards, including blocking by technical identifiers and integrating automated tools in generative AI to prevent the spread of harmful content.

we call for the implementation of enhanced blocking mechanisms, allowing users to block-not only specific usernames or phone numbers-but also associated IP addresses or any other technical identifiers that could be used to create alternate accounts for harassment or unwanted contact.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Warns of the dangers of over-blocking by automated filters, highlighting the need not to undermine minors' right to information.

We are concerned that automated content or search filters (as proposed in line 568 ff.) will lead to over-blocking, as demonstrated by a recent example from the United States.

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Recommends using labelling or signaling for legal but potentially harmful content, rather than removal.

Finally, some content may be legal but could be potentially harmful to certain user groups too (e.g., based on usage patterns and recommendations). In such cases, content should not be removed, but measures such as labelling or signaling (by trusted flaggers, for example) could be implemented.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Advocates creating a continually updated, multilingual registry of high-risk terms to help platforms keep pace with evolving risks.

Create and maintain a continuously updated, multilingual registry of high-risk terms (e.g. harmful slang, emojis, hashtags), curated by the EU Centre for Algorithmic Transparency.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recommends restricting features like autocomplete for children, using AI moderation, and collaborating with helplines to adapt safeguards against emerging risks.

Autocomplete and suggested terms should be completely turned off depending on the evolving capacities of children as there is the potential for to recommend harmful content or be addictive.

Microsoft response to the European Commission's draft 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 (Microsoft). Calls for clearer guidance on the application of technical solutions to prevent AI from facilitating access to harmful content, acknowledging the diversity of AI integration.

Finally, we note the requirement on page 26 to "implement technical solutions to prevent the Al system on their platform from allowing users to access, generate, and disseminate" content harmful to minors.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Supports use of advanced technologies, like machine learning and hash-matching, combined with human oversight, to detect and mitigate exposure to harmful content.

Thorn strongly supports the recommendation to use advanced technologies to detect and prevent dissemination of and exposure to harmful content, particularly sexual exploitation and grooming.

Børns Vilkårs Comments on the Commission’s Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Emphasizes the importance of robust AI mechanisms to limit and label misinformation and disinformation in content accessed by minors.

we urge the Commission to explicitly address the risks of misinformation and disinformation in AI-generated content accessed by children.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Suggests automated detection and blocking of previously reported/deleted harmful content to prevent re-uploads.

Mögliche Maßnahme: automatisierte Erkennung von den bereits gemeldeten und gelöschten Inhalten und anschließende Blockierung dieser für den erneuten Upload.

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 (European Commission). Directs platforms to deploy effective technical solutions and mechanisms to proactively reduce minor’s exposure to harmful content, including blocking dangerous search terms and suggestions.

Put in place effective technologies, internal mechanisms and preventative features to reduce the risk of content and behaviour that are harmful to minors' privacy, safety of security from being shown to minors in their accounts' interface or other functionalities of the service, including:

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Critiques the use of automated block lists or filters for search features, arguing it could restrict minors' access to essential information.

Similarly, we are concerned that suggested limitations to search and discovery features through automated block lists or filters (lines 568 - 573).

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Urges that AI chatbots should be prevented from providing advice on sensitive topics without adequate safeguards.

This means that for instance AI chatbots should not be able to provide advice or guidance on sensitive topics without appropriate safeguards, testing and clear limitations.

Input from the ECA to the Guidelines on protection of minors online under the Digital Services Act (European Casino Association (ECA)). Highlights the need for algorithmic moderation to distinguish between regulated and illegal gambling, to avoid undue restrictions on lawful operators.

While the European Commission acknowledges the issues related to these (illicit) contents and practices on online platforms, there is a tangible risk that automated moderation or advertising restriction tools, if not properly managed, may inadvertently classify content from regulated casino operators alongside high-risk illegal gambling content, leading to undue restrictions and lower consumer trust in safe, legal options.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Argues for the responsible use of behavioral data to enhance child safety, with clear safeguards, purpose limits, and transparency.

The emphasis should be on purpose limitation, transparency, and data minimization-not on excluding valuable tools that, if properly managed, contribute directly to risk mitigation and user wellbeing.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). Proposes real-time content flagging and alerts as protective measures, in lieu of exclusion mechanisms.

We suggest providing measures to flag up potentially harmful content directly as it is being seen by the minor; e.g. pop-ups after a phone number has been posted or certain buzzwords were written.

1.5.6 Contextual and Cultural Adaptation

The insights under 'Contextual and Cultural Adaptation' emphasize the importance of tailoring content moderation and harm prevention measures to account for cultural, contextual, linguistic, and service-specific differences across EU member states. There is a strong push for moving beyond one-size-fits-all approaches—such as prescriptive catalogues or fully automated moderation—towards measures that reflect local language nuances, lived realities, and offline standards regarding what constitutes harm for minors. Multiple contributors stress that the guidelines should require more human moderation with cultural and contextual awareness, age-appropriate and culturally sensitive educational materials, transparency in moderation priorities, and safeguards that are consistent across all member states and adapt to evolving terminology. Concerns are also expressed about vague content categories leading to overblocking, and about the need to ensure that online protection is at least as rigorous and nuanced as offline equivalents. Overall, moderation should recognize vulnerability differences (e.g., gender, ethnicity, disability), avoid overgeneralization, and provide children with tools and definitions they can understand, regardless of their background or language. The adaptability and transparency of such measures are seen as key to effectively protecting minors online while respecting freedom of expression and access to information.

Bris also wishes to emphasize the importance of assessing what may constitute harmful content for children in an extensive manner, considering cultural and contextual differences. (Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris))

What is considered harmful content varies between contexts. Bris therefor emphasizes the importance of ensuring that content moderation can address the linguistic, cultural, and contextual differences that

exist across EU member states. (Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris))

Ensure that children wherever they are and whatever language they speak are constantly protected by moderation practices. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Bris believes this must be more clearly reflected in the guidelines and must also account for the fact that content which is not illegal may still be highly inappropriate for children. (Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris))

We are concerned that measures aimed at preventing minors' exposure to potentially risky content (lines 551 - 561) could lead to overblocking and restrictions of the freedom of expression and access to information. (Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation))

A related issue is that these measures have to be implemented across all languages for the different member states. (European Commission Article 28 Guidelines Feedback (unknown))

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Argues that content moderation strategies should be adjusted to fit the unique characteristics of different online services, especially when dealing with encrypted environments.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Highlights the need for guidelines to explicitly recognize cultural and contextual diversity in defining harm for children and advocates for more human moderation with such awareness.

What is considered harmful content varies between contexts. Bris therefor emphasizes the importance of ensuring that content moderation can address the linguistic, cultural, and contextual differences that exist across EU member states.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Recommends that platforms provide age-appropriate and culturally sensitive definitions and examples in reporting tools so children from varied backgrounds can understand and report complex abuse.

In addition to offering clear and accessible reporting tools, platforms should provide age-appropriate and culturally sensitive examples and definitions that clearly explain what these forms of abuse entail.

Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance). Suggests that online content regulation should reflect existing offline standards, and calls for a proportionate, risk-based approach to ensure effective and realistic protection.

We encourage the Commission to align online content regulation with offline norms.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Emphasizes the need for moderation practices that account for vulnerabilities based on identity factors and for transparency in moderation prioritization.

Providers should also take into account if harmful content may exploit the vulnerabilities of children, especially in terms of gender, sexual orientation, disability or ethnical background.

Microsoft response to the European Commission's draft 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 (Microsoft). Urges a nuanced understanding of disinformation risk due to its variable nature and calls for diverse, platform-appropriate responses.

We also note that the references to disinformation risks may not adequately reflect the variability of manifestations for this particular harm type and the consequent variability in platform-appropriate mitigations.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Warns against vague and culturally insensitive content categories that risk overblocking, and calls for removal of such references.

Vague categories like "promoting unrealistic beauty standards" (line 553) ignore that what content is appropriate for minors can vary depending on cultural norms and the person in question.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Stresses the importance of ensuring consistent and language-inclusive online protection for all children.

Ensure that children wherever they are and whatever language they speak are constantly protected by moderation practices.

European Commission Article 28 Guidelines Feedback (unknown). Advocates for adaptable safeguards at the search index level that respond to changing language and usage, ensuring equal protection in all member state languages.

Basic testing done earlier this year showed that on Instagram, searches for some of the most basic terms in Spanish did not get any of the promised protections.

1.5.7 Protection of Minors and Vulnerable Users

The insights across these documents reflect a strong consensus on the need for robust and nuanced measures to protect minors and vulnerable users online. Core principles include a child-rights-centered and risk-based approach that recognizes the diverse and evolving risks children face—from exposure to harmful, illegal, or age-inappropriate content, to grooming, exploitation, and privacy violations. The guidelines under Article 28 of the DSA highlight the necessity for platforms to adopt proactive strategies such as visible warning messages, age-appropriate content classification, reporting and support mechanisms, and age assurance. There is also call for flexible yet enforceable benchmarks, holistic consideration of criminal risk, specific protections for particularly vulnerable user groups, and the mitigation of risks from new technologies like generative AI. Documents further emphasize that a one-size-fits-all solution is insufficient; differentiated responses tailored to the type of content, platform function, and the nature and severity of potential harm to minors are advocated. Concerns are raised about unintended negative impacts from overly broad suppression laws and the need to balance protection with the rights and autonomy of minors. Special consideration is given to the importance of supporting minors encountering harm (even if not policy-violating), avoiding stigmatization, and ensuring that protections do not restrict beneficial digital participation or free speech.

In particular, An Coimisiún welcomes that the draft guidelines adopt and promote a child-centred, rights- based perspective that, among other things, recognises children as subjects of rights and that the best interests of the child must be a primary consideration in all actions relating to them. (Public consultation on 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 (Coimisiún na Meán))

Introduce directly visible warning messages, links to relevant national support lines and other authoritative sources when minors search for, upload, generate or share content that is potentially illegal or harmful. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

In addition, based on detailed examination of targeted safeguards to children and a dataset of 313,740 content moderation decisions on Discord, TikTok, and YouTube, this research proposes four policy considerations to improving privacy, safety, and security of minors on social media (B1–B4). (Salminen contribution protection of minors (Aalto University))

Further, due to the inherent tradeoffs caused by segregate-and-suppress laws, the laws inevitably harm some minors. (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

A high false positive rate for such messages could mean they are not taken seriously or risk alienating minors. (Microsoft response to the European Commission's draft 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 (Microsoft))

We commend the Guidelines' focus on preventing repeated exposure to content that could be detrimental to minors. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

Public consultation on 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 (Coimisiún na Meán). Advocates for a child-centered, rights-based approach to online safety, ensuring the best interests of children are central in platform design and media regulation.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Suggests direct warning messages and national support links for minors exposed to harmful content, alongside strengthened features to block, mute, or report such material.

Introduce directly visible warning messages, links to relevant national support lines and other authoritative sources when minors search for, upload, generate or share content that is potentially illegal or harmful.

Salminen contribution protection of minors (Aalto University). Calls for targeted safeguards and policy measures on social platforms to improve minors' privacy and safety, citing insufficient current moderation and age verification.

In addition, based on detailed examination of targeted safeguards to children and a dataset of 313,740 content moderation decisions on Discord, TikTok, and YouTube, this research proposes four policy considerations to improving privacy, safety, and security of minors on social media (B1–B4).

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Highlights the need for platforms to address algorithmic and content-driven risks to children's mental health and prevent repeated harmful exposure.

TikTok fails to address risks to children and young people's mental health despite past warnings",

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Recommends prohibiting public distribution of sexually explicit content without explicit consent, prioritizing minors' protection from exploitation.

Prohibit the public distribution of sexually explicit content depicting individuals who do not explicitly provide permission.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Calls for bans on public distribution of non-consensual sexually explicit content, relevant to protecting minors from such abuses.

Prohibit the public distribution of sexually explicit content depicting individuals who do not explicitly provide permission.

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Reports high rates of children encountering disturbing content, urging platforms to enforce more effective protective mechanisms.

62% of children in 7th grade and 34% of children in 4th grade have seen disturbing content.

ACT RESPONSE TO THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Association of Commercial Television and Video on Demand in Europe (ACT)). Urges audiovisual platform alignment by making minor-protection measures and basic content ratings mandatory for VSPs to ensure age-appropriateness.

Rating system (AVMSD Art. 28b(3)(g)): While traditional content rating systems (e.g. for VoD and TV programmes) may not be feasible given the volume of user-generated content, platforms should at least implement basic rating mechanisms that enable users and guardians to assess content based on age-appropriateness

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Advises on preventing minors' repeated exposure to harmful or distressing content, including content that impacts body image, mental health, or safety.

Implement measures to prevent a minor's repeated exposure to content that could pose a risk to minors' safety and security, particularly when encountered repeatedly, such as content promoting unrealistic beauty standards or dieting, content that glorifies or trivialises mental health issues, such as anxiety or depression, discriminatory content, illegal content and distressing content depicting violence or encouraging minors to engage in dangerous activities."

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Advocates for clear terms of service and user-friendly content rating systems to protect minors from harmful programming and communications.

We would like to point out that VSPs are also equally obliged to include in their terms of services requirements foreseen in the AVMSD that they protect minors from programmes, user- generated videos and audiovisual commercial communications which may impair their physical, mental or moral development, as well as the public, including minors from incitement to violence and hatred and content the dissemination of which constitutes acriminal offence under Union law.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Supports full implementation of guidelines by platforms to shield minors from harmful content, manipulative design, and exploitation.

If these guidelines are fully implemented by the digital platforms, they while play a key role in strengthening minors in the digital environment, protecting them from harmful content, unwanted contact, manipulative designs and commercial exploitation.

Policy_demands (unknown). Encourages expanding the scope of regulated harms to minors beyond pornography/gambling to include self-harm, violence, and discriminatory content.

Other forms of harmful content, including content promoting violence, self-harm, disordered eating, or discriminatory behaviour (e.g., misogyny or anti-LGBTQI rhetoric), are well- documented risks to minors and need to be included.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Proposes blurring private messages containing potentially age-inappropriate, pornographic, or violent images to let minors opt in if appropriate.

Blurring of private messages with potentially age inappropriate content as well as potentially pornographic or violent images, which can be optionally unblocked by users by clicking on them.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Advises a harm-based, rather than identity-based, approach to prioritizing user reports for better protection outcomes for minors.

While the intention to protect minors is crucial, the prioritisation of user reports under Article 28 should not rest on the identity of the person submitting the report. Instead, the determining factor should be the nature and severity of the harm described in the report, particularly where the harm poses risks to the privacy, safety, or well-being of minors.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Recommends evaluating content moderation effectiveness and prioritizing seriousness of harm, not just incident scale, in response to threats to minors.

although the number of minors potentially being affected is an important consideration to prioritise content moderation, the seriousness of the incident, even if it only affects a limited number of children, may be more important in some cases.

Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children). Calls for robust safeguards in generative AI to detect and block prompts and outputs that endanger minors.

Generative AI systems should integrate stringent safeguards that detect and prevent both inputs (prompts) and outputs that harm minors.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Seeks consistent but context-sensitive approaches to restricting minors' access in online marketplaces, distinguishing between explicit content and general products.

while it is appropriate to restrict explicit sexual content from being displayed to minors, this logic should not be extended to products, which are not inherently inappropriate to be viewed.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Stresses the need to clarify obligations for high-risk platforms and ensure exemptions do not compromise protection where risks to minors are high.

recommend that the guidelines: . Explicitly clarify that the exemption for small and micro enterprises should not apply to platforms whose services pose high risks to minors, such as those hosting or disseminating pornographic content;

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 (BeSmartOnline! Maltese Safer Internet Centre). Advocates for integrating criminal prevention with user protection, addressing adults exploiting or victimizing minors online.

A more comprehensive approach must also address the criminal misuse of platforms by adults who target and victimize minors.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Argues for a holistic approach to children's online safety, treating them as both users and potential victims of exploitation.

However, to adopt a holistic approach to the threats facing children online, it is essential to think of minors not just as the subject-actor of their online surfing, but also as the subject-victim of actual pedocriminal practices from which they must be protected.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Critiques 'segregate-and-suppress' regulatory models, warning they may inadvertently harm some minors and risk free speech.

In other words, segregate-and-suppress laws seek to protect minors online by harming minors online.

Public consultation on the protection of minors' guidelines under the Digital Services Act (Telefónica S.A). Urges for tools and robust measures enabling minors to detect and avoid dangerous interactions, including adults posing as children.

Provide minors with the necessary tools to identify and avoid potentially dangerous interactions with adults who register on a platform posing as minors.

STATEMENT (Digipeace (Digirauha ry)). Pushes for enforceable anti-grooming benchmarks and protection for minors featured in harmful content, not just users.

The Guidelines should set forth clear, enforceable benchmarks that specifically target and mitigate risks of grooming and sexual exploitation to ensure that digital platforms consider these dangers as one of their priorities in mitigating risks minors face on their platforms.

COMMENTS FROM ESYS ON THE PUBLIC CONSULTATION REGARDING 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 (ESYS Foundation). Advocates differentiated policy tailored to type of content (gambling, adult, disinformation) for effective child protection under the DSA.

Different types of content should be considered independently and distinctly. Gambling, adult content (pornographic material), alcohol or tobacco sales are not the same as disinformation or cyberbullying. These are fundamentally different activities from both a legal and risk management perspective and therefore require differentiated policy measures.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Warns basic AI warnings are insufficient for protecting minors from AI-generated misinformation or manipulation, and additional safeguards are needed.

Simply notifying minors that they are interacting with AI systems does not adequately address the risks of AI-generated misinformation or emotional manipulation, both of which can have serious impacts on children's mental well being and decision-making processes.

Statement - DSA Guidelines (Protect Children). Calls for explicit benchmarks and robust privacy/age assurance to prevent grooming, sexual exploitation, and address real dangers of online abuse.

Online platforms should implement clear, enforceable benchmarks that specifically target and mitigate risks of grooming and sexual exploitation, ensuring that online platforms consider these dangers as a priority.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recommends feedback functions be private to users to prevent their misuse in bullying or harassing minors on platforms.

COFACE welcomes that providers of online platforms should ensure that feedback options are designed in such a way that they are only visible to the user, so that they cannot be misused by others to bully or harass minors on the platform (line 751-754).

Feedback DSA (unknown). Proposes immediate hiding of flagged inappropriate content from minors until reviewed, and the addition of age-appropriate trigger warnings and safety labels.

Inappropriate content flagged by users should be immediately hidden from minors until reviewed and manually approved by human moderators.

Microsoft response to the European Commission's draft 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 (Microsoft). Supports minor-focused support features but calls for platform flexibility regarding when and where to display help and warning links.

However, we note that there are some limitations with this proposal that could be acknowledged in the Guidelines, including to ensure that online platforms have the flexibility to determine where and at what point information should be provided on external support to ensure any "warning measures" or links to authoritative sources are deployed to address identified high-risk scenarios.

Børns Vilkårs Comments on the Commission’s Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Highlights the digital vulnerabilities of children in alternative care, urging explicit coverage in DSA protections.

We therefore encourage the Commission to explicitly address the needs of children in alternative care as part of a broader focus on children in vulnerable situations.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Emphasizes measures to prevent repeated harmful content exposure, especially around body image, mental health, and safety risks to minors.

Implement measures to prevent a minor's repeated exposure to content that could pose a risk to minors' safety and security, particularly when encountered repeatedly, such as content promoting unrealistic beauty standards or dieting, content that glorifies or trivialises mental health issues, such as anxiety or depression, discriminatory content, illegal content and distressing content depicting violence or encouraging minors to engage in dangerous activities."

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Favors preventing repeated exposure to harmful content and notes YouTube's steps to disperse such viewership among teens.

YouTube, for example, has proactively implemented safeguards to disperse viewership of such content for teens.

Guidelines to ensure high levels of privacy, safety, and security for minors online (Kaspersky). Urges additional, child-friendly reporting tools to address online grooming and abuse effectively.

We would like to draw particular attention to measures aimed at mitigating the risks associated with online grooming.

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 (European Commission). Calls for immediate visible warning messages and referral links for support when minors encounter or report potentially harmful content.

roduce directly visible warning messages, links to relevant national support lines (59) and other authoritative sources when minors search for, upload, generate or share content that is potentially illegal or harmful for the privacy, safety and security of minors

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Stresses detecting, labeling, and moderating AI-generated content to prevent manipulation and to ensure appropriate guidance for minors.

the comments highlight the imperative to detect and label AI-generated content, such as synthetic videos or audio, to prevent manipulation and misinformation.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Reminds that VSPs must implement protective measures for minors against specific content types according to relevant audiovisual regulation.

Recall that online platforms that are VSPs, have to put in place measures in order to protect minors from specific type of content in line with article 28b(1) of the AVMSD.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Calls for proactive, proportionate app and platform-led actions to shield minors from harmful or age-inappropriate content.

Ultimately, we call for apps and platforms to do more to ensure the protection of minors safety, security and privacy as they best placed to take targeted and proportionate action to prevent minors from accessing content which is harmful or age inappropriat

Contribution from medical professionals regarding the Draft Commission Guidelines on the Protection of Minors Online (Article 28 DSA) (Youth Smoking Prevention Foundation (Stichting Rookpreventie Jeugd); #vapenjouwkeuze). Raises concern about the illegal marketing of vapes to minors via social platforms and calls for explicit regulatory intervention.

This forms a serious and unacceptable threat to children’s health, and the Commission should explicitly address this issue in the Guidelines.

Input from the ECA to the Guidelines on protection of minors online under the Digital Services Act (European Casino Association (ECA)). Stresses the need for stricter protections against illegal gambling content targeting minors and other vulnerable groups.

minors and vulnerable consumers should be protected against illegal and non-age-appropriate content, including those related to gambling.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Recommends balancing risk likelihood and harm impact, not just the number of affected minors, in content moderation priorities.

Take into account the following factors when prioritising moderation: the likelihood of the content causing harm to a minor's privacy, safety and/or security, the impact of the harm on that minor, and the number of minors who may be harmed.

European Commission Article 28 Guidelines Feedback (unknown). Highlights frequent harmful encounters for minors even when unintentional, calling for experiential support as well as content moderation.

So it is essential to support the minor with what they experience to be harmful content, or harmful contact.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Advocates for scientifically-based, graduated content ratings and age classifications as part of children's protection online.

1.5.8 Addictive and Manipulative Design Features

The insights in this category focus on identifying, regulating, and mitigating design features in digital platforms that are addictive or manipulative, particularly for minors. Key strategies include targeting prevention efforts at at-risk groups for gaming and gambling addiction, developing and enforcing clear policies against dark patterns and engagement-maximizing algorithms, and ensuring transparency for gambling-like features such as loot boxes. There is strong emphasis on integrating concrete, mandatory guidelines—such as friction in sharing, disabling features that promote overuse, and banning manipulative or persuasive design for minors. Several documents stress the adaptation of protections from the traditional gambling sector, including age restriction and self-limitation tools, for digital environments. Calls for robust regulation are coupled with concerns that current guidelines may be too vague or cosmetic, risking the persistence of addictive platform structures. Advocates recommend explicit recognition of risks like overexposure, algorithmic bias, and the psychological triggers embedded in many features. The importance of proportionate moderation, safeguarding child autonomy, and restricting exploitative systemic designs—such as AI simulating empathy—are highlighted as essential to preventing behavioral addictions and associated harms in minors.

Deceptive tech designs, also called "dark patterns," manipulate or mislead people to behaviors in the interest of tech companies rather than those using the platform. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

ensure that "minors are not exposed to practices that can lead to excessive or unwanted spending or addictive behaviours, by ensuring that virtual items such as loot boxes, other products with random or unpredictable outcomes or gambling-like features are not accessible to minors, and by introducing separation or friction between content and the purchasing of related products" (Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE))

features that may contribute to excessive use, such as the number of "likes" or "reactions", communication "streaks", the " ... is typing" function, ephemeral content, and "read receipts," are turned off. (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 (European Commission))

Antisocial Media: How Facebook Disconnects Us and Undermines Democracy. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

exercise of moderation should be proportionate to the extent of the identified tolerable risks as stated in the guidelines. (IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)))

n este sentido, la Comisión Europea conoce el estudio "Loot boxes in online games and their effect on consumers, in particular young consumers"2, encargado por Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo, en el que se llama la atención sobre los diferentes riesgos asociados a los mecanismos de las cajas botín en función de la fase de desarrollo de los niños, y de acuerdo con el cual, estos serían los principales factores de riesgo en el desarrollo de niños y adolescentes (INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego))

What do you bet? (Que t'hi jugues) (Catalan Audiovisual Council (CAC)). Highlights the need to target prevention strategies towards risk groups prone to gaming and gambling addiction, focusing on demographic and cognitive factors.

Age (the older the age, the greater the risk) and the degree of cognitive distortion associated with gambling (the greater the mastery of gambling, the greater the bias) are risk factors for developing addictive behaviour.

Salminen contribution protection of minors (Aalto University). Emphasizes further investigation and regulation of addictive platform features to promote children's mental and physical health, outlining key policy strategies.

The study outlines three key policy considerations (A1–A3) aimed at promoting the mental and physical health of children by addressing platform features associated with behavioral addiction.

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). Supports more comprehensive guidance on dark patterns affecting minors, especially in the gaming sector, and advocates for detailed platform-specific best practices.

Since Article 25 remains quite broad, we would suggest using the present opportunity to explore dark patterns and minors' protection more thoroughly, and to provide practical "dos and don'ts" for platforms, particularly in the gaming sector.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Discusses how deceptive design, or dark patterns, exploit psychological biases, and recommends policy measures to counteract such manipulative algorithms.

Deceptive tech designs, also called "dark patterns," manipulate or mislead people to behaviors in the interest of tech companies rather than those using the platform.

Safe by Default (Panoptykon Foundation). Recommends introducing friction into sharing mechanisms (e.g., changing reshare buttons) and nudges to prevent hasty or uncritical content sharing by users.

Changing the reshare button is a proven solution",

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Stresses the importance of restricting access to loot boxes and other gambling-like digital features for minors, and requiring transparency when such features are available.

ensure that "minors are not exposed to practices that can lead to excessive or unwanted spending or addictive behaviours, by ensuring that virtual items such as loot boxes, other products with random or unpredictable outcomes or gambling-like features are not accessible to minors, and by introducing separation or friction between content and the purchasing of related products"

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Argues for the banning of manipulative design elements targeting minors and calls for mandatory protective standards with effective enforcement.

Only mandatory standards with real consequences will protect minors online.

Feedback DSA (unknown). Urges platforms to avoid promoting content related to self-harm, eating disorders, or suicidality to minors, and to direct young users to relevant support resources instead.

Should explicitly avoid recommending content related to self-harm, eating disorders, or suicidality.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Critiques current guidelines as insufficiently concrete for addiction prevention and calls for clear technical requirements, mandatory safety features, and dedicated oversight.

Ohne klare technische Anforderungen, verpflichtende Schutzfunktionen, Monitoringmechanismen und pädagogische Begleitung besteht das Risiko, dass suchtgefährdende Strukturen bestehen bleiben oder nur „kosmetisch“ verändert werden.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Advocates for applying established gambling protection measures, such as self-limitation and strict age restrictions, to simulated gambling within games.

Spiele, die simuliertes Glücksspiel beinhalten, sollten erst für Personen ab dem vollendenten 18. Lebensjahr freigegeben werden.

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 (European Commission). Recommends default disabling of features that drive excessive platform use or negatively impact minors' mental health, including likes, streaks, and harmful filters.

features that may contribute to excessive use, such as the number of "likes" or "reactions", communication "streaks", the " ... is typing" function, ephemeral content, and "read receipts," are turned off.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Calls for clear identification of overexposure and extensive screen use as risks in policy guidelines, ensuring providers recognize and assess these hazards.

Explicitly include among the risks identified by the guidelines the issue of overexposure, that is, the extensive or excessive use.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Requests clarification and proportionality in guidelines targeting inauthentic notifications, possibly referring to dark patterns and click-bait techniques.

TikTok also requests clarification on what "notifications should never be inauthentic" means in practice. We understand this may relate to dark patterns or 'click-bait', but would welcome greater clarity on the expectation here.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Highlights the need for moderation techniques that strictly prohibit manipulative design patterns and prioritize child autonomy and consent.

Risks associated with manipulative design patterns e.g. dark patterns, and safeguarding child agency and consent should not be a tolerable risk.

INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego). Reiterates the necessity of robust enforcement against exposing minors to loot boxes and similar addictive features, with recommendations for more stringent separation and regulation.

> *Ensure that minors are not exposed to practices that can lead to excessive or unwanted spending or addictive behaviours, by ensuring that virtual items such as loot boxes, other products with random or unpredictable outcomes or gambling- like features are not accessible to minors, and by introducing separation or friction between content and the purchasing of related products."*

The Case Against AI Simulated Empathy (unknown). Warns against AI systems simulating empathy, arguing that such features exploit psychological vulnerabilities and undermine authentic relationships.

> *AI systems should not display empathy-like responses because they exploit our fragmented identities and liquid relationships to provide the appearance of connection without its substance.*

1.5.9 Miscellaneous

1.6 Platform and System Design for Child Safety

Systemic and proactive responsibility by platforms and ecosystem actors is widely recognized as the cornerstone of effective child online safety. Key insights emphasize that safety, privacy, and wellbeing for children should be embedded as the default—"not optional"—setting across all digital systems, shifting accountability from individual users or parents onto platforms themselves. Regulatory frameworks, such as the EU Digital Services Act (DSA), are seen as crucial in driving enforceable standards, backed by robust governance structures, compliance through regular oversight, and alignment with clear codes of conduct and age-appropriate design specifications. A common thread across categories is the necessity for transparency and independent, regular evaluation of platforms' protective measures, including explicit, actionable guidelines and clear communications tailored to minors. Strong advocacy persists for active prevention of manipulative or addictive design features—such as infinite scroll or algorithmic loops—ensuring these are either banned or disabled by default for young users, while remaining mindful of proportionality and sector-specific needs. Content moderation and access controls should restrict unsolicited adult contact, limit discoverability, and employ tiered, trauma-informed interventions, supported by harmonised industry practices and independent certifications. Child-centered, age-appropriate environments must prioritize the best interests and developmental needs of minors, balancing safety, autonomy, and participation through flexible, inclusive design and positive empowerment. Regular adaptation of safeguards in response to new risks is recommended, alongside clear distinctions between privacy, safety, and commercial interests in interface design. Overall, there is consensus that collaborative, multi-layered strategies—combining regulation, technical solutions, industry standards, and participatory approaches—are essential for establishing a safe, supportive digital ecosystem for children.

1.6.1 Platform and Ecosystem Responsibility

The 'Platform and Ecosystem Responsibility' category is centered on the need for digital platforms, device manufacturers, telecom providers, and other ecosystem actors to assume proactive, uniform, and systemic responsibility for protecting children online. Insights emphasize that platforms must design their systems, algorithms, and business models with child safety as a core priority, with protective measures and age-appropriate safeguards implemented by default and not left to parental intervention alone. There is strong advocacy for extending protective obligations beyond just major platforms to the entire tech ecosystem, including smaller entities, OS and browser developers, and edtech tools, to ensure consistency and close gaps exploited by harmful actors. Several documents call for regulatory and industry-wide standards such as default child-friendly service plans, accessible parental controls, and consistent thresholds for safety requirements regardless of platform size. There is an insistence that exemptions for small or micro businesses undermine effectiveness, as these services can also expose children to significant risks. The importance of regular platform updates based on new risks, local adaptability, and universally applied minimum standards is also highlighted. Finally, the collaborative role of platforms, policymakers, and third parties (like OS developers) is seen as vital to ensure robust, enforceable protections for children.

> *Telecom providers should offer child-friendly service plans, restrict unfiltered access to harmful content by default, and provide clear, accessible tools for guardians to manage children's data use, screen time, and app access.* (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

> *Platforms must be held responsible for ensuring that search functionality and recommender systems are designed and maintained to actively prevent minors from being exposed to harmful or age-inappropriate content at all times.* (Consultation Submission Summary: Strengthening Platform

Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España))

We support the framing that children are rights holders, and that platform accountability and responsibility must not be offloaded to parents or guardians alone. (Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation))

The proposed guidelines indicate that providers should design default settings to ensure that "No account, except the minor's, can download or take screenshots of content uploaded or shared by the minor to the platform" (line 400). (Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children))

We support the framing that children are rights holders, and that platform accountability and responsibility must not be offloaded to parents or guardians alone. (Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation))

Adjusting the design and functioning of the aforementioned elements based on the results of these consultations and on technical developments, research, changes in user behaviour or policy, product and usage evolutions, and changes to the harms and risks to the privacy, safety and security of minors on their platform. (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 (European Commission))

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Advocates for extending digital child protections to include the entire device and service ecosystem, urging that telecoms and tech providers supply child-friendly plans and restrictions as defaults.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Recommends mandatory child-friendly telecom service plans, default content restrictions, and that protective obligations encompass all tech and device providers in the ecosystem.

Telecom providers should offer child-friendly service plans, restrict unfiltered access to harmful content by default, and provide clear, accessible tools for guardians to manage children's data use, screen time, and app access.

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Calls for making platforms fully accountable for age-appropriate design, especially in algorithmic content curation and search, to prevent minors' exposure to harmful content.

Platforms must be held responsible for ensuring that search functionality and recommender systems are designed and maintained to actively prevent minors from being exposed to harmful or age-inappropriate content at all times.

Ten recommendations to the European Commission to really protect children online (unknown). Proposes mandatory telecom service plans catered to children, default safeguards against harmful content, and requiring device manufacturers to offer parental controls by default.

Telecom providers should offer child-friendly service plans, restrict unfiltered access to harmful content by default, and provide clear, accessible tools for guardians to manage children’s data use, screen time, and app access.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Recommends that platforms enable prosocial governance and local adaptability, and that foundational child safety and data protection responsibilities be obligatory for fair competition.

To be inclusive and effective, deliberative tools must be adaptable to different cultural, linguistic, and ethical contexts.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Highlights Apple's commitment to building in tools like Screen Time and Communication Safety, and making them available to third-party developers to enhance child safety.

Apple is proud of our industry-leading innovations, including Screen Time and Communication Safety, that help keep children safe on our devices while honoring our commitments to the other rights of our users.

Ten recommendations to the European Commission to really protect children online (unknown). Emphasizes the need for telecom providers to offer child-friendly plans, default content filters, accessible parental controls, and broader obligations for the digital ecosystem.

Telecom providers should offer child-friendly service plans, restrict unfiltered access to harmful content by default, and provide clear, accessible tools for guardians to manage children's data use, screen time, and app access.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). Welcomes platform responsibility for risk assessment and tailored protections for minors, advocating for platforms to apply proportionate mechanisms based on their specific user base.

Nous saluons la reconnaissance explicite, par la Commission, du rôle central des plateformes dans la mise en œuvre d'outils efficaces de protection des mineurs, notamment pour l'évaluation des risques, le paramétrage des algorithmes, la conception d'interfaces adaptées, ou encore les dispositifs de signalement des contenus préjudiciables.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Argues that platforms must take complete responsibility by adapting their designs, algorithms, and business models to prioritize children's rights and needs.

Bris emphasises that this potential requires digital platforms to take full responsibility and proactively adapt their design, algorithms, and business models with the rights and needs of children as the primary consideration.

Policy_demands (unknown). Seeks to expand safety obligations beyond platforms to include device makers and telecoms, critiquing a narrow regulatory focus.

Extend protective obligations to the broader tech ecosystem, including device manufacturers, telecom providers, and education tech platforms.

Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children). Highlights technical challenges in enforcing child safety defaults due to reliance on device and OS manufacturers, calling for cross-ecosystem cooperation.

This may require some technically compatible engineering by OS developers and/or device manufacturers to grant apps the ability to disable screen capturing/recording functions on the device.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Supports design-centered safety strategies, emphasizing platform accountability and that responsibility must not be offloaded solely onto parents.

We support the framing that children are rights holders, and that platform accountability and responsibility must not be offloaded to parents or guardians alone.

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 (BeSmartOnline! Maltese

Safer Internet Centre). Warns against exempting micro and small enterprises from obligations, expressing concern that this limits the effectiveness of child protection frameworks.

Paragraphs 82-86 exempt micro and small enterprises from compliance, which undermines the framework's protective reach.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Stresses the need for clear standards, longevity in commitments, and shared responsibility for children's online safety across platforms of all sizes.

As digital environments continue to evolve rapidly, ensuring children's safety online will require not only ambitious guidance but also clear implementation standards, long-term commitments, and shared responsibility across all platforms, regardless of size.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Calls for all digital services accessible to minors to be subject to minimum protections, regardless of company size or legal status.

It is essential to broaden the scope of the guidelines to cover all digital services accessible to minors, regardless of their size or legal status.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Endorses the focus on platform accountability and service design as key factors in risk and responsibility for child safety online.

We support the framing that children are rights holders, and that platform accountability and responsibility must not be offloaded to parents or guardians alone.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Urges for mandatory, enforceable safeguards such as reporting and blocking tools, and consistency in protections across platforms and devices.

For systemic protection of children in digital environments, key safeguards such as access to support tools and the ability to block users must be mandatory rather than discretionary.

Børns Vilkårs Comments on the Commission’s Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Maintains that online services for minors should proactively integrate child rights into their design, algorithms, and business models.

However, this potential can only be realised if online services accessible to minors assume responsibility and proactively align their design choices, algorithms and business models with the rights and needs of children.

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 (European Commission). Advocates for ongoing improvement of design and functionality in response to stakeholder input, research, and evolving risks to minors.

Adjusting the design and functioning of the aforementioned elements based on the results of these consultations and on technical developments, research, changes in user behaviour or policy, product and usage evolutions, and changes to the harms and risks to the privacy, safety and security of minors on their platform.

Feedback for 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 (xHamster). Asserts that protective measures should not depend on company size but apply equally across all services for effective child safety.

When protecting children is the goal, the size of the service should not matter.

Ten recommendations to the European Commission to really protect children online (unknown). Recommends child-friendly telecom plans with default protections and parental controls, proposing reforms to the prevalent always-on data commercial model.

Telecom providers should offer child-friendly service plans, restrict unfiltered access to harmful content by default, and provide clear, accessible tools for guardians to manage children's data use, screen time, and app access.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Suggests industry-wide mandatory defaults for safety settings to ensure consistent protection standards.

We suggest that the guidelines mandate industry-wide defaults for key settings to ensure consistency across platforms.

Overall feedback on the Commissions guidelines on measures to ensure a high level of privacy, safety and security for minors online (ECPAT Sweden). Argues against exemptions for small and micro enterprises, noting such platforms can still play a substantial role in child safety risks.

With regards to the exemption for micro and small enterprises set out on line 82-86 of the communication, we want to stress that even small and medium sized enterprises can have significant negative impact on child safety online, particularly when it comes to the dissemination of child sexual abuse material.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Highlights the current lack of child-appropriate telecom products and calls for industry support for parents in protecting children online.

Telecombedrijven bieden vrijwel geen 'gepaste' producten aan om kinderen te beschermen.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Emphasizes default safeguards in telecom offerings and calls for an expansion of protective obligations to include the entire digital ecosystem.

Telecom providers should offer child-friendly service plans, restrict unfiltered access to harmful content by default, and provide clear, accessible tools for guardians to manage children's data use, screen time, and app access.

INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego). Suggests that protective measures for minors online should be expanded to benefit the general public as well.

En su documento la Comisión anima a las plataformas en línea a extender las medidas propuestas más allá del ámbito estricto de los menores de edad (menores de 18 años), sino al público consumidor en general.

1.6.2 Governance, Accountability, and Regulatory Alignment

This category addresses the governance, accountability, and regulatory alignment aspects of platform and system design for child safety, especially in the context of the EU Digital Services Act (DSA) Article 28. The insights consistently advocate for robust, enforceable standards and continual regulatory oversight to ensure children's online safety. Key recommendations include establishing dedicated governance structures (such as child safety officers), fostering industry-wide cooperation, and implementing clear, reviewable codes of conduct centered on age-appropriate design. There is strong support for the adoption and alignment with existing frameworks (like AFNOR SPEC 2305 and CWA 18016/IEEE 2089) to standardize protections, reduce compliance risks, and prevent unsafe or addictive designs. Several documents emphasize proactive, child-centric design philosophies, advocating for involvement of interdisciplinary experts, holistic approaches (combining regulation, education, and technical solutions), and the expansion of guidelines to cover all platforms accessible

to minors, in keeping with the broader aims of the EU Charter of Fundamental Rights. Overall, the insights point to a multi-layered governance ecosystem characterized by periodic review, proactive industry obligations, and a fundamental prioritization of children's rights and well-being within platform and system design.

> *Minimum building standards ensure that all companies adhere to the same rules, preventing unfair competition and protecting consumers from unsafe platforms.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))
>
> *tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.* (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation))
>
> *Vodafone supports the call for dedicated governance structures within platforms to oversee child safety.* (Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group))
>
> *Companies, investors, governments, and the public need ways to measure both antisocial and prosocial impacts alongside growth and profit.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))
>
> *The work of the European Commission on a code of conduct on age appropriate design should be continued.* (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))
>
> *It is worth noting that all provisions of the DSA, including Article 28, need to be read in the light of primary EU law, especially Article 24 of the EU Charter of Fundamental Rights on the rights of the child.* (Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Advocates for industry-wide cooperation and further platform design modifications under the DSA to reduce technology addictiveness and enhance children's safety.

Stellungnahme zur öffentlichen EU Konsultation: Leitlinien der Kommission für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre und Sicherheit für Minderjährige im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022 / 2065 (Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg). Calls for the legal definition and regulation of addictive design to improve governance and accountability in protecting minors online.

süchtig machende Designs legal zu definieren,

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Proposes prosocial platform governance and metrics to align platform impact with social cohesion and regulatory requirements under the DSA.

A price signal for social cohesion could measure and reward prosocial outcomes like empathy, trust, and civic participation.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Recommends enforceable minimum tech design standards to ensure platform safety and compliance, reducing risks and strengthening accountability.

Minimum building standards ensure that all companies adhere to the same rules, preventing unfair competition and protecting consumers from unsafe platforms.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Suggests appointing child safety officers in Digital Services Coordinators and embedding minors-focused chapters in platforms' codes of conduct.

appoint child safety officers or focal points.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Urges the continuation of the EU's initiative on codes of conduct for age-appropriate digital design as a regulatory anchor.

The work of the European Commission on a code of conduct on age appropriate design should be continued.

Safe by Default (Panoptykon Foundation). Highlights the need for enhanced regulation and consumer protection mechanisms addressing addictive design, with special focus on children and youth.

report on addictive design of online services and consumer protection in the EU single market

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Recommends integrating AFNOR SPEC 2305—a pre-existing collaborative standard for minors' protection—into DSA implementation.

ndeed, the AFNOR SPEC 2305 for "Risk prevention and protection of minors on social media platforms"1 is the result of a collaborative project involving a group of experts in the fields of social media, online safety and child protection.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Advocates for incorporating CWA 18016 on age-appropriate digital services and for setting structured review periods for DSA guidelines.

tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Emphasizes the need to continue developing the code of conduct for age-appropriate design and implementing a clear, recurring guideline review process.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recommends ongoing work on the EU's code of conduct for age-appropriate design for sustained regulatory improvement.

The work of the European Commission on a code of conduct on age appropriate design should be continued.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Stresses the involvement of developmental psychologists and addiction prevention experts to guide interdisciplinary platform design supervision.

Es gibt auch keine Empfehlungen zur interdisziplinären Begleitung von Plattform-Design (z. B. durch Entwicklungspsychologen oder Suchtpräventionsexperten).

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Calls for the guidelines to be broadened to all platforms accessible to minors to ensure equal protection across the EU.

In order to ensure the same level of protection for all minors in the EU, it is essential that all online platforms where children are present, adhere to the guidelines.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Urges

interpretation and application of all DSA provisions, especially Article 28, in favor of maximal child protection consistent with the EU Charter of Rights.

Thus, the default interpretation of any provision of the Guidelines should be in favor of more, rather than less, protection of minors.

Joint Statement on Article 28 Guidelines (5Rights Foundation). Supports the EU's ongoing development of a code of conduct for age-appropriate design as an accountability mechanism.

The work of the European Commission on a code of conduct on age appropriate design should be continued.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Endorses the establishment of dedicated internal governance structures for child safety within digital platforms.

Vodafone supports the call for dedicated governance structures within platforms to oversee child safety.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Advocates integrating WHO guidelines on screen time and age-specific content into child safety regulation at multiple governance levels.

De Wereldgezondheidsorganisatie heeft leeftijdsnormen vooropgesteld rond schermgebruik, leeftijdsspecifieke inhoud etc.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Promotes holistic and consistent enforcement of DSA requirements for child-appropriate design, including media education and provider responsibility.

There is a need for child-appropriate design (see Child Rights by Design) and consistent implementation of legal requirements such as the Digital Services Act (DSA), which provides important guidelines for online platform providers.

1.6.3 Transparency and Oversight

The category 'Transparency and Oversight' within Platform and System Design for Child Safety emphasizes the necessity for clear, specific, and actionable guidelines to ensure minors' safety on digital platforms. A recurring theme is the call for extending precise service design standards, as exemplified in Section 6 of certain Guidelines, across all regulatory sections to ensure effective and equitable child protection. Key insights highlight the need for greater transparency in platforms' terms and conditions, ensuring they comprehensively communicate account processes and community conduct expectations tailored to minors. To facilitate oversight, there is strong advocacy for regular, preferably annual, independent third-party reviews of key protections like default settings. Stakeholders also stress the importance of unambiguous criteria for platform accessibility to minors, as well as clearer distinctions among provisions focused on privacy, safety, security, and different age groups. Altogether, these views reinforce the belief that robust, transparent, and externally validated processes are vital to improving both compliance and real-world outcomes for children's safety online.

This model should be extended across all sections to ensure that the Guidelines provide the comprehensive, actionable direction necessary for meaningful compliance and equitable protection for all children. (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

The guidelines clarify that excluding minors based on the terms and conditions of an online platform would not be enough, effective measures are required to avoid minors accessing the service. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

We ask for clarification on the definition of 'regular' in relation to categorising and monitoring default settings, and recommend this review is mandated annually across platforms by an independent third party. (Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group))

ore clarity is needed on what makes a platform not accessible to minors, to help service providers understand whether their services fall in scope of Article 28 DSA or not. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

We contend that the precision and specificity demonstrated in Section 6 offers a good benchmark in terms of the detail of guidance provided to platforms that should be applied throughout the Guidelines. (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

The guidelines clarify that excluding minors based on the terms and conditions of an online platform would not be enough, effective measures are required to avoid minors accessing the service. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Advocates for the extension of precise, actionable guidance on service design, demonstrated effectively in Section 6, to all sections of the guidelines to ensure comprehensive and consistent protection for minors.

This model should be extended across all sections to ensure that the Guidelines provide the comprehensive, actionable direction necessary for meaningful compliance and equitable protection for all children.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Highlights the need for clearer criteria regarding accessibility to minors, to help platforms determine their obligations under Article 28 DSA and ensure more effective exclusion of underaged users where appropriate.

The guidelines clarify that excluding minors based on the terms and conditions of an online platform would not be enough, effective measures are required to avoid minors accessing the service.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Calls for clearer differentiation and purpose-setting within the guidelines governing default settings, emphasizing distinctions between privacy, safety, security, and age appropriateness for minors.

In the discussion of default settings on pages 16 and 17, it appears that much of the age- appropriate design code has been incorporated. This code valuably underpins privacy, safety, and the child's best interests; however, in the many provisions required by these guidelines, no clear distinctions are made between provisions for privacy, safety, security, or different age groups. Greater clarity as to the purposes to be achieved by particular provisions is needed.

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 (European Commission). Emphasizes that terms and conditions should transparently communicate both account management processes and community guidelines tailored for a safe and inclusive environment for minors.

eation to its deletion. o Community guidelines that promote a positive, safe and inclusive atmosphere and that explain what conduct is expected and prohibited on their service, and what the consequences of non-compliance are.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Recommends mandating annual, independent, third-party reviews of default settings for minors to ensure consistent, transparent oversight across platforms.

We ask for clarification on the definition of 'regular' in relation to categorising and monitoring default settings, and recommend this review is mandated annually across platforms by an independent third party.

1.6.4 Safety, Privacy, and Wellbeing by Default

The insights in this category emphasize that platforms and systems must prioritize child safety, privacy, and wellbeing by implementing safety, privacy, and wellbeing features as default—not optional—settings. Responsibility shifts from users and guardians to platforms, underscoring legal and ethical obligations for safety-by-design, systemic accountability, and child-centric interfaces. Recommendations focus strongly on

private-by-default accounts, restricting unsolicited adult contact, minimizing discoverability, and disabling visibility and sharing of personal content and performance metrics for minors unless actively chosen otherwise. Stakeholders advocate for measures such as privacy-preserving age assurance tools, periodic resetting of settings to safe defaults, limitations on addictive design and commercial exploitation, and holistic digital wellbeing support for young users. Importantly, many submissions stress practical steps like blocking screenshots of minors' content, requiring explicit consent for activating sensitive features, and embedding default safeguards at both device and software levels. Flexible, graduated protections that adapt to user age and maturity, as well as extending protective defaults system-wide when differentiation is not possible, are also championed. Training and vetting for staff interacting directly with children, and transparency in design and algorithms, further support a proactive, comprehensive approach. Safety, privacy, and wellbeing by default are framed as a baseline, not an aspiration, for children's rights in the digital environment.

> *Legal obligation to maintain age-appropriate search and recommendation settings by default, with accountability for failures.* (Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España))
>
> *What we hope is that, at the end of this process, (very large) social media platforms will have strong incentives to join a race to the top: competing with each other for default settings that prioritise safety and quality in user experience, and prototyping advanced features that allow for independent curation of recommended content.* (Safe by Default (Panoptykon Foundation))
>
> *Examples of features that may put minors' privacy, safety or security at risk include, but are not limited to, enabling location sharing, switching to a public profile, allowing other users to view their contact or follower lists, allowing sharing of media files, and hosting or participating in a live stream.* (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 (European Commission))
>
> *This requires a systemic shift in responsibility, whereby platforms-not minors, not parents, not regulators-carry the onus to design, test, and maintain environments that default to safety.* (Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España))
>
> *These are vital steps toward creating fairer and more just digital spaces.* (Securing a high level of privacy, safety and security for minors online (SUPERRR Lab))
>
> *Cette communication, par un message textuel ou par une vidéo, devra permettre d'assurer un temps de réflexion à l'adolescent sur ses usages des réseaux sociaux.* (Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)))

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Calls for legal obligations to ensure age-appropriate settings are default and platforms themselves are fully accountable for design and enforcement failures regarding children's safety online.

Salminen contribution protection of minors (Aalto University). Proposes a novel unmeasurable-by-default design for child accounts to hide performance metrics and mitigate psychological pressures linked to visible social feedback for minors.

> *This study advocates for the implementation of a "unmeasurable–by–default" design principle for child accounts to reduce the reliance on quantifiable feedback and help mitigate the psychological pressures associated with social media use among younger audiences.*

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Recommends prioritizing safety-by-design over age verification methods, and ensures any necessary age assurance is done in privacy-preserving ways.

Given the inevitability of collecting and processing personal data, we recommend that greater emphasis be put on design choices that platform providers can make to increase safety-by-design as opposed to implementing age assurance/verification and increasing data collection.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Advocates for strict safety-by-design mandates for platforms as required by the EU Digital Services Act, embedding child safety in technological governance.

Trust & Safety Professional Association. "Implementing Safety by Design." In Trust & Safety Curriculum.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Emphasizes that platforms should recognize a range of prevention measures, especially robust default settings and proactive steps to prevent unwanted contact with minors.

Add measures we line out in other parts of this response in more detail as equally effective to reach a high threshold for safety, security and privacy of minors online (e.g. on default settings, measures to prevent unwanted contact with minors).

Safe by Default (Panoptykon Foundation). Encourages platforms to make safety and high-quality experiences competitive, innovating default settings and features that proactively protect children.

What we hope is that, at the end of this process, (very large) social media platforms will have strong incentives to join a race to the top: competing with each other for default settings that prioritise safety and quality in user experience, and prototyping advanced features that allow for independent curation of recommended content.

Additional contribution (Collective Shout). Highlights the need for platforms to proactively address grooming and child exploitation by implementing additional, default safety features.

In line with our #wakeupinstagram campaign, we recommend an additional focus on grooming and exploiting children on social media networks.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Advocates for technological protections like screenshot blockers and anti-copy features to safeguard children's images and prevent digital violence.

inors must be protected from harmful image and video content, for example by mak- ing it unrecognisable. At the same time, user-generated image and video content from minors must be protected from misuse.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Stresses the importance of personal integrity and recommends applying maximum protective default settings to unregistered users, presuming they may be minors.

Protecting the personal integrity of minors is a key obligation for all stakeholders involved in modern child and youth protection in the media.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Recommends mandatory child safeguarding training and background checks for staff in direct contact with minors on digital platforms.

However, they do not explicitly mention that team members who are in direct contact with children should undergo child safeguarding training and background checks, in line with Directive 2011/93/EU ("Employers when recruiting for a post involving direct and regular contact with children are entitled to be informed of existing convictions for sexual offences against children entered in the criminal record, or of existing disqualifications.").

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 (BeSmartOnline! Maltese Safer Internet Centre). Suggests stringent privacy and safety defaults for minors, including private mode, prevention of unsolicited adult contact, screenshot prevention, and curbing addictive design elements.

The proposed default settings demonstrate a deep understanding of the risks embedded in platform design.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Urges default settings that genuinely reduce structural and behavioral risks for minors, explicitly including screenshot prohibition on minors' content.

The recommendations on default settings reflect a genuine desire to reduce exposure to systemic risks arising from platform design.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Advocates for minors' accounts to be invisible and private by default, allowing only approved contacts access; unapproved interactions are blocked by design.

minors' profiles must be configured by default as invisible to unknown users and that any content they publish should only become accessible after an explicit approval of a contact request.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Calls for smart, age-appropriate default settings that support both the safety and autonomy of children across different age groups.

Children's safety and autonomy must be supported through smart defaults.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Recommends restricting unsolicited contact from adults, limiting minor account discoverability, and requiring explicit opt-in for sensitive features to majorly mitigate online abuse risks.

By default, platforms should prevent minors from receiving unsolicited messages, friend or follower requests, or comments from users they do not know, particularly from adult accounts, unless the child has deliberately chosen to enable those interactions.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Recommends that default safety and privacy mechanisms for minors be maintained and, where feasible, extended to all users to reinforce protections.

We support the Guideline's encouragement for platforms to adopt protective measures for all users, not just minors.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Proposes platform design that inherently supports privacy, transparency, accessibility, and digital wellbeing for minors as fundamental operating principles.

The guidelines propose general principles that should govern all measures for providers to ensure privacy, safety, and security for minors.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Suggests that after temporary changes to a child's settings, platforms should auto-reset these to safe defaults, reducing accidental overexposure.

If children adjust settings in a single session, those changes may persist longer than intended or be forgotten. An auto-reset mechanism ensures temporary adjustments don't expose minors to ongoing risks.

Feedback DSA (unknown). Recommends private accounts by default, nighttime use deterrents, and irreversible bans on downloads or screenshots of minor accounts to limit exposure.

Ensure minors' accounts are set to private by default.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Calls for all minor accounts to be equipped with robust default content and feature protections, especially to prevent unsolicited adult contact.

comptes configurés par défaut pour les mineurs, avec des mesures de protection activées à la fois pour le contenu et les fonctionnalités (par exemple, la désactivation de la possibilité, pour des adultes inconnus, de contacter des mineurs)

Microsoft response to the European Commission's draft 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 (Microsoft). Supports strongest feasible privacy and safety defaults for minors, with flexibility to tailor gradations by age, platform type, and risk profile.

We support the general proposition that minor accounts should consistently have the strongest privacy and safety protections available, depending on the service, and the age of the child (for example, it may be appropriate to have graduated settings for older teens).

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Recommends default account setup that prevents minors from being automatically added to groups on registration, to reduce unsolicited exposure.

Weiters sollte ein Account/Registrierung „per default“ so eingestellt sein, dass jugendliche Nutzer:innen nicht automatisch Mitglied in einer Gruppe sind (siehe dazu auch Zeile 836 der Leitlinien).

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 (European Commission). Enumerates risky features and underlines the importance of high-level default protections that can be tailored across a range of ages and needs.

Examples of features that may put minors' privacy, safety or security at risk include, but are not limited to, enabling location sharing, switching to a public profile, allowing other users to view their contact or follower lists, allowing sharing of media files, and hosting or participating in a live stream.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Argues for default settings as a baseline safety net and advocates against the use of retention mechanisms that exploit or endanger minors.

Ensure that minors are not exposed to retention mechanisms and addictive designs and make use of default settings to ensure a baseline of safety for minors;

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Stresses platform responsibility for developing minor-specific default parameters that balance reducing risk and safeguarding fundamental rights.

Afin de réduire les risques auxquels les mineurs sont exposés en ligne (voir la classification des 5C), il incombe aux plateformes de mettre en place des paramètres spécifiques concernant la conception et le fonctionnement de leurs services.

Ten recommendations to the European Commission to really protect children online (unknown). Pushes for device-level, not just app-level, child protections and for manufacturers to offer pre-installed, default child-specific safety controls.

Device manufacturers should be required to offer child-specific settings, including pre-installed safety tools, usage tracking, and meaningful parental controls as default.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Urges moving beyond simple harm prevention to promoting digital wellbeing and broader developmental support for minors by default.

In addition to preventing specific categories of harm, governance frameworks should adopt a holistic and modern approach that includes additionally the promotion of digital well-being.

Joint Statement on Article 28 Guidelines (5Rights Foundation). Welcomes a shift to designing privacy, safety, and security as underlying principles for all platforms, rather than reacting to risks after they occur.

we welcome the clear focus on the design of online platforms and the inclusion of safety, security and privacy by design as a general principle.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Appreciates explicit safety-by-default guidelines for minors and calls for clear specification of the required protective measures.

We highly acknowledge that the guidelines include guidance on how to increase safety by design and by default for minors on online platforms.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Supports outcome-based, risk-informed account settings that emphasize default safety configurations such as contact and data sharing restrictions.

Default safety settings such as limiting contact, visibility, and data sharing remains a central pillar of our platform design and policy for protecting Younger Users.

On the concept of personal integrity in the german protection of minors (unknown). Frames safety and privacy by design as essential to respecting the best interests of the child, providing practical guidance for protective digital environments.

These safety by design and privacy by design approaches are therefore essential prerequisites for ensuring that the best interests of the child are prioritised in the digital world.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Extends the safety-by-design principle to the development, deployment, and lifecycle of AI systems, recommending technical safeguards against child abuse.

EEE P3462TM Recommended Practice for Using Safety by Design in Generative Models to Prioritize Child Safety follows a safety by design approach by providing recommendations for developing, deploying, and maintaining generative artificial intelligence models with adequate safeguards against child sexual abuse.

POLICY PAPER BY GERMAN CIVIL SOCIETY ORGANIZATIONS ON THE SUBJECT OF AGE VERIFICATION / AGE ASSURANCE (Kinderschutzbund Bundesverband e.V. (German Child Protection Association) and SUPERRR Lab). Proposes that users unwilling to verify age on age-graded services should still have access via a maximally secure default settings profile.

Those who do not wish to have their age verified or determined should be able to use the service in the most secure setting, provided that the service offers age-graded content and/or functions.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). States that, if practical, safety measures intended for minors should be operationalized for all users to maximize protective coverage.

Wir begrüßen die Klarstellung, dass eine sichere Online-Umgebung für alle Nutzerinnen und Nutzer auch die Sicherheit von Kindern und Jugendlichen stärkt.

1.6.5 Child-Centered and Age-Appropriate Design

The collective insights on Child-Centered and Age-Appropriate Design emphasize the need for online platforms to tailor digital environments, features, and content to the diverse developmental, cognitive, and emotional needs of children and young people. Central recommendations include designing online experiences specifically for distinct age groups, prioritizing children's best interests and safety, and avoiding one-size-fits-all technical solutions. Many submissions advocate for design flexibility that accounts for platform type, size, and risk profile, as well as personalized safeguards that evolve with the growing capacities of minors. Stakeholders highlight the importance of explicit standards and clear evaluation methods for implementing age-appropriate design, often calling for dedicated annexes or codes of conduct within policy frameworks. There is a strong consensus that platform and system design should balance safety, privacy, participation, and mental health, and avoid manipulative patterns that exploit minors' vulnerabilities. Several contributions stress child-centered default settings, accessible interfaces, and the inclusion of participatory and inclusive design considering diverse backgrounds, abilities, and experiences. Overall, there is broad agreement that guidelines should be proportionate, practicable, and foster innovation while ensuring robust child protection by design.

Age-appropriate design: providers of online platforms accessible to minors should design their services to align with the developmental, cognitive, and emotional needs of minors, while ensuring their safety, privacy, and security (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 (European Commission))

The guidelines should support the best interests of children, balancing privacy, safety, mental health, access to information, and freedom to participate. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

As a general recommendation, CCIA Europe calls on the Commission to make sure that the final guidelines are proportionate and flexible enough, allowing platforms to tailor design choices to guarantee minor protection in a way that best fits their respective services. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

We appreciate the recognition of the best interest of the child as a guiding principle. However, we recommend that the Commission provide more specific guidance on what constitutes best interests in digital contexts, rather than delegating this to providers. (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))

As long as a trader can substantiate their claim, they should be allowed to communicate to users that their products are soon to be out of stock. (Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe))

Kinder und Jugendliche nutzen das Interface nicht wie Erwachsene. (Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)))

Innovative age assurance: Email address as the new benchmark for frictionless age estimation (Verifymy). Recommends creating digital experiences and environments explicitly tailored for specific age groups, restricting cross-age communication where needed to enhance safety and appropriateness.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates for clear guidance on system-level changes, including incorporating health risk protection for children during account registration and grounding responsibility in international child rights standards.

The focus on system design is a breakthrough in the context of digital policy, putting the responsibility on online platforms in line with UN General Comment No. 25.

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Urges that search engines, recommender systems, and platforms must fundamentally serve the best interests of minors as a moral and regulatory obligation, not merely an accommodation.

We call on the Commission to adopt a firm stance: search engines, recommender systems, and platform design must always serve the best interests of minors-not merely accommodate them.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Calls for detailed age-appropriate design considerations to be included in a separate annex for better clarity and implementation guidance.

Detail considerations relating to age appropriate design as mentioned under section 4 and as referred to in several sections in a separate annex;

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Stresses the need for flexibility and balance in age-appropriate design, supporting measures that align privacy, safety, and access to information with the best interests of children, rather than prescriptive mandates.

The guidelines should support the best interests of children, balancing privacy, safety, mental health, access to information, and freedom to participate.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Encourages proportionate and flexible age-appropriate design guidelines that allow platforms to tailor protection measures based on their service offerings rather than following prescriptive technical rules.

As a general recommendation, CCIA Europe calls on the Commission to make sure that the final guidelines are proportionate and flexible enough, allowing platforms to tailor design choices to guarantee minor protection in a way that best fits their respective services.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Emphasizes prioritizing children's rights in European digital policy and placing them centrally in age-appropriate design and system principles.

Bris welcomes the emphasis in the guidelines on the importance of considering all of the child's rights under the UNCRC.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Recommends risk-minimizing, target group-oriented design and default settings to address minors' susceptibility to manipulative design and support safer online navigation.

Minors are a particularly vulnerable target group since they are more susceptible to manipulative design due to their lim- ited experience, cognitive development, and higher emotional responsiveness.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Argues that protection of minors guidelines should be adapted based on platform size and available resources, offering scalable compliance pathways for smaller companies.

Different sized companies will inherently have different levels of resources available to them as a whole, and so we'd recommend creating more of a spectrum of expectations and options for smaller companies to use and still be in compliance with the guidelines.

DSA_Article_28_GitHub_Response (GitHub). Suggests acknowledging that the requirements for age-appropriate design may vary on specialized, less youth–oriented platforms, reducing unnecessary burdens where minor risks are low.

We recommend that the Guidelines more clearly acknowledge that age-appropriate may vary for more specialized platforms.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Recommends clear guidance on distinguishing principal services from minor functionalities, particularly for online games, and regulating particularly intrusive designs targeted at minors.

The exact delimitation between the principal service and minor functionalities is still in need of clarification.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Appreciates focus on children's best interests but warns against interpretations of proportionality that could dilute protections in favor of commercial interests; suggests clearer guidance for age-appropriateness.

The current framing of proportionality may be interpreted as a loophole, potentially weakening protective measures in favour of commercial interests.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Advocates for explicit clarification that account and default setting rules should specifically refer to minors' accounts for accurate classification and enforcement of protective measures.

There is also no explicit clarification that the requirements in section 6.3.2 ("Account Settings") expressly refer to accounts belonging to minor

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Encourages more nuanced, practical examples tailored for gaming platforms to demonstrate effective, participatory risk mitigation through design.

We would welcome the addition of more nuanced, gaming-specific illustrations that demonstrate proactive risk mitigation, embedded safety features, and participatory design.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Argues for flexible adaptation of interface design practices, like infinite scrolling, to different platforms rather than imposing blanket bans due to minor protection concerns.

This is a narrow-viewed approach that must be tailored to the specific service in question.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Calls for explicit recognition of children's diversity in design measures and advocates for a detailed annex dedicated to age-appropriate design in guidelines.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Recommends an annex defining standards for age-appropriate design with clear developmental benchmarks to help platforms translate child rights into design decisions.

Introduce an annex detailing standards for age-appropriate design that include design benchmarks tailored to developmental stages, and support platforms in translating the child rights framework into concrete product choices.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Urges continuation of developing a code of conduct on age-appropriate design and the addition of a detailed annex to DSA guidelines for more specific guidance.

The work of the European Commission on a code of conduct on age appropriate design should be continued.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Suggests graduated default settings by age group, simplified communication for minors due to attention limits, and integrating user experience and latency considerations into technical standards.

Providers should adopt a graduated approach to default settings, calibrated by age groups (e.g., under 13, 13-15, 16-17), ensuring that younger children benefit from stricter safeguards.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Recommends detailing age-appropriate design considerations in a separate annex for clearer, actionable guidance.

Detail considerations relating to age appropriate design as mentioned under section 4 and as referred to in several sections in a separate annex;

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Emphasizes child-friendly and non-manipulative registration and account processes, with enforced information about age restrictions and avoidance of dark patterns.

Providers should ensure that the registration process does not nudge children into sharing more information than required or adapting their settings in less privacy- preserving ways and does not include any dark patterns.

Microsoft response to the European Commission's draft 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 (Microsoft). Advocates for linked development of age assurance and robust, clear standards for creating age- and child-centered online experiences based on user age ranges.

We recommend that in parallel to developing age assurance solutions, the Commission also seeks to introduce clear standards for providers to create child-centered experiences tailored based on age ranges.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Calls for differentiated user interfaces for children and recommendations for designs with reduced stimulation and risk elements tailored to younger users' needs.

ennoch gibt es keine differenzierte Gestaltung nach Altersstufen in den Leitlinien, zB reduzierte Reizdichte, kein Multi- Tasking-Modus, abgeschwächte Animationen je nach Alter, keine Glücksspielelemente sowie glücksspielähnlichen Elemente, keine Gewalt, uvm wären empfehlenswert.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Urges proportionate design standards that consider developmental differences among minors, and a focus on delivering enriching, age-appropriate digital content.

This appears to be at odds with the Commission's aim that providers "design their services to align with the developmental, cognitive, and emotional needs of minors, while ensuring their safety, privacy, and security".

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 (European Commission). Articulates the core requirement for platforms accessible to minors to design for developmental, cognitive, and emotional needs of children while ensuring safety, privacy, and security.

Age-appropriate design: providers of online platforms accessible to minors should design their services to align with the developmental, cognitive, and emotional needs of minors, while ensuring their safety, privacy, and security

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Emphasizes allowing flexibility in the application of protective measures and presenting information in accessible formats to avoid information overload for minors.

Platforms should maintain the flexibility to design their services in a way that offers protective measures without compromising the overall user experience or creating information fatigue among minor users through excessive notifications and warnings.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Describes national efforts to establish EU-wide standards for age-appropriate design and effective age verification, including a proposed digital age of majority for social media access.

Greece advanced a set of proposals aimed at establishing a pan-European digital age of majority for social media access and creating binding technical standards for age-appropriate, child-friendly app design.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Advocates for 'child safety-by-design' to be embedded into internal policies for all new platform features, ensuring safeguards are proactively built into products.

We encourage the Commission to include that internal policies that outline how the provider of the online platform seeks to ensure high level of privacy, safety and security for minors on its service include 'child safety-by-design' for all new feature and product development.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Urges the establishment of a clear definition and robust evaluation methods for age-appropriate design to accurately assess compliance.

We therefore urge the Commission to define age-appropriate design and establish clear evaluation methods to determine when a design meets these criteria.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Encourages innovation and proportionality in protective measures, supporting tailored protections for children under 18 rather than limiting access entirely.

The guidelines should remain open to innovation and ensure measures taken by platforms are tailored to the nature, characteristics, community of users, and content of the platform.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Supports maximizing safety and privacy through default settings, with flexibility for platforms to adapt experiences according to a child's age and the service's risk profile.

We support the principle that default settings should maximise safety and privacy for children.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Recommends the continued development of a code of conduct and a separate annex for detailed age-appropriate design guidance within the DSA framework.

The work of the European Commission on a code of conduct on age appropriate design should be continued.

On the concept of personal integrity in the german protection of minors (unknown). Highlights the need for age- and developmentally appropriate protective measures that also support children's access to information and participation rights without overprotection.

The legal obligation to protect the personal integrity must fulfilled in a way that does not close off access to information and allows the expression of opinions and participation in political decision-making processes in an age- and development-appropriate manner.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Advises including a dedicated annex in guidelines for age-appropriate design and supporting an ongoing code of conduct for the same.

Detail considerations relating to age appropriate design as mentioned under section 4 and as referred to in several sections in a separate annex;

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Stresses the importance of flexibility for platforms to tailor safety measures based on specific risks and service context rather than following a prescriptive model.

Flexibility for platforms to tailor measures based on service-specific risks and capabilities;

DSA (Protection of Minors) Guidelines (Samsung Electronics). Suggests guideline updates for logical user experiences and better accommodation of shared devices, fostering effective minor protection.

Overall, SE believes the Guidelines should be updated to ensure both logical user experiences and greater consideration for shared devices.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Argues that default platform settings should be graduated by age cohort, and recommends embedding 'Fairness by Design' as a core design principle alongside safety and privacy.

In diesem Zusammenhang sollte jedoch auch dem Gedanken der stetig wachsenden Fähigkeiten von Minderjährigen Rechnung getragen werden.

1.6.6 Mitigation of Manipulative and Addictive Features

A strong consensus emerges across these documents that manipulative and addictive design features targeting minors must be explicitly banned or strictly regulated on online platforms. These features—such as infinite scroll, autoplay, algorithmic content loops, Snapstreaks, gamification elements, and exploitative notification systems—are repeatedly identified as drivers of excessive screen time, compulsive engagement, and associated harms for children and teenagers. There is a wide call for the Digital Services Act (DSA) and related guidelines to specifically prohibit or deactivate such features by default for users under 18. Recommendations extend beyond bans, advocating for supportive measures such as intelligent break suggestions, default deactivation of high-risk features, enhancement of user agency through friction and reflection prompts, and age-appropriate design. Several contributions also emphasize the necessity for clearer definitions and categorization of persuasive design, a reduction in harmful choice architecture, and the provision of accessible tools for minors to control their experience and mitigate risks. While a minority of stakeholders caution against overly prescriptive or friction-heavy mandates, the prevailing view is that protection—not retention or engagement—must be paramount in platform and system design for children's online safety.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Ensuring that minors are not exposed to persuasive design features that are aimed predominantly at engagement or that may lead to extensive use or overuse of the platform or the forming of problematic or compulsive behavioural habits. (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 (European Commission))

Dabei könnten klare Gestaltungsrichtlinien, verpflichtende Nutzungspausen, Vermeidung von Glücksspielelementen, Gamification-Reduktion und Reflexionstools entscheidend zur digitalen Resilienz junger Nutzer:innen beitragen. (Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)))

Friction deliberately adds barriers to prevent antisocial behaviors on platforms. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Design practices (e.g. dark patterns) that encourage minors to reduce their privacy or increase visibility should be expressly prohibited, in line with the principle of child-appropriate design. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

The guidelines should provide clear definitions of such design features and explicitly prohibit their use for minors. (Ten recommendations to the European Commission to really protect children online (unknown))

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Advocates for an explicit ban on manipulative design features such as infinite scroll, autoplay, and algorithmic loops for users under 18 to reduce exposure to excessive screen time and harm.

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Recommends the deployment of intelligent break suggestion algorithms that identify natural transition points in user engagement to encourage healthier usage patterns among minors.

Deploy intelligent break suggestion algorithms that identify natural transition points in user engagement (such as between videos, after completing game levels, or at the end of content series) to suggest breaks.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Calls for an explicit prohibition of manipulative design features tailored for under-18s, highlighting their risks for excessive digital consumption.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

TOP 21 Verbot von Tracking, Verhaltensanalysen und Profilbildung zu Werbezwecken (personalisierter Werbung) (Verbraucherschutzministerkonferenz). Urges rigorous enforcement and stricter regulation of manipulative and addictive interface designs—particularly under the DSA—to ensure consumer protection.

Die Verbraucherschutzministerinnen, -minister und -senatorinnen der Länder bitten den Bund, sich auf EU-Ebene dafür einzusetzen, die Überprüfung von Online-Plattformen und sozialen Netzwerken hinsichtlich des Verbots manipulativer oder süchtig machender Gestaltungen im Sinne des Digital Services Act konsequent und nachhaltig umzusetzen.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Recommends default deactivation of features potentially harmful to minors' body image and mental health, and stresses the importance of curbing persuasive and manipulative design.

filters functionalities, including filters, that can have detrimental effects on body image, self- esteem and mental health are turned off by default.

Ten recommendations to the European Commission to really protect children online (unknown). Seeks an explicit ban on manipulative designs for under-18s, emphasizing their role in harmful overuse.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

Stellungnahme zur öffentlichen EU Konsultation: Leitlinien der Kommission für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre und Sicherheit für Minderjährige im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022 / 2065 (Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg). Supports the strict

implementation of bans on manipulative and addictive design practices, especially dark patterns that deeply engage minors.

das Verbot manipulativer und süchtig machender Designs, insb. High Engaging Dark Patterns bei der Anwendung des Digital Service Act () konsequent umzusetzen, da es insbesondere einen regelrechten Sog für Kinder und Jugendliche erzeugt,

CONCLUSION & POLICY DEMANDS (unknown). Demands explicit prohibition under the DSA of manipulative platforms targeting those under 18.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Proposes implementing purposeful friction in platforms to slow down antisocial behaviors and foster user reflection, particularly on encrypted services.

While most designs aim to reduce friction for engagement, purposeful friction in ethical technology design can promote reflection and minimize harm.

Ten recommendations to the European Commission to really protect children online (unknown). Again calls to ban manipulative design elements for minors, naming specific engagement-increasing features.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

Safe by Default (Panoptykon Foundation). Highlights the need to counteract misleading and addictive design in social media and user interfaces as a child safety measure.

Recent studies discussing consequences of misleading design in user feedback settings:

Policy_demands (unknown). Presents a policy demand to prohibit manipulative features like infinite scroll and autoplay for minors.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

DOT Europe response1 (DOT Europe). Cautions against over-reliance on friction or nudging in design, emphasizing alignment with the DSA's spirit of fairness and non-deception.

while Article 25 DSA bans online interface designs which "deceive or manipulate" users, I. 418, 442, 444 and 498 recommend online platform providers to create as much friction as possible in the experience of users.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Evidence shows all major platforms use high-engagement dark pattern elements, especially those driving FOMO and compulsive behaviors; recommends banning such features for children.

Particu- larly striking techniques included infinite scroll, autoplay, gamification, and the ex- ploitation of the "fear of missing out" (FOMO).

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Supports strong default settings to disable compulsive and privacy-threatening features for minors, including notifications, streaks, and autoplay.

These include disabling features known to encourage compulsive use or compromise privacy, such as push notifications, geolocation tracking, camera access, location sharing, public visibility, autoplay, streaks, and read receipts.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Recommends an immediate ban on manipulative design features in online platforms.

Ban on manipulative design features

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Encourages the Commission to clarify the distinction between persuasive design patterns fostering compulsive usage and voluntary excessive use among minors.

It would be useful to clearly distinguish between 'excessive use' via the users own volition and design that intentionally undermines user agency.

Public consultation on the protection of minors' guidelines under the Digital Services Act (Telefónica S.A). Suggests disabling infinite scroll and imposing time limits for minors to encourage autonomous, healthier tech decisions.

Suggestion: Disable infinite scrolling by default on accounts belonging to minors.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Advocates for default limiting of design features that drive increased time and compulsive platform use by minors, such as autoplay and streaks.

limiting by default design features that encourage or increase the frequency, time spent, or activity of minors on the covered platform, such as infinite scrolling, auto playing, rewards for time spent on the platform, notifications, and other design features that result in compulsive usage of the covered platform by the minor;

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Argues for a ban on manipulative design that nudges minors toward reduced privacy and improper engagement defaults.

Although asking minors to confirm or modify choices represents a positive step, some platforms may exploit this as a loophole to nudge children toward privacy-eroding behaviours.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Stipulates that platforms must avoid features like infinite scroll and algorithmic feedback loops that promote compulsive use amongst minors.

Platforms must avoid infinite scroll, autoplay, and algorithmic feedback loops that encourage compulsive use among minors.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Suggests clear guidelines requiring mandatory breaks, reflection prompts, and reduction of gamified or gambling-like elements for youth resilience online.

Dabei könnten klare Gestaltungsrichtlinien, verpflichtende Nutzungspausen, Vermeidung von Glücksspielelementen, Gamification-Reduktion und Reflexionstools entscheidend zur digitalen Resilienz junger Nutzer:innen beitragen.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Recommends mandatory warning messages and deactivation of autoplay for child-focused video content.

Eine Möglichkeit wäre beispielsweise auch Autoplay für solche Inhalte zu deaktivieren.

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 (European Commission). Underlines the need to avoid persuasive design features that induce compulsive use or problematic habits in minors and lists specific practices to eliminate.

Ensuring that minors are not exposed to persuasive design features that are aimed predominantly at engagement or that may lead to extensive use or overuse of the platform or the forming of problematic or compulsive behavioural habits.

Ten recommendations to the European Commission to really protect children online (unknown). Echoes the shared call to explicitly ban manipulative design features for minors.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Highlights that child protection is incompatible with engagement-obsessed design and advocates for success metrics that value disengagement opportunities.

Protecting minors cannot coexist with the relentless pursuit of engagement through persuasive, status-driven design.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Encourages precise definitions and evidence reviews related to harmful choice architecture and persuasive online design.

See, e.g., Busch and Fletcher, "Harmful Online Choice Architecture"; Competition and Markets Authority, "Evidence review of Online Choice Architecture and consumer and competition harm"; Fletcher, "Choice Architecture for End Users in the DMA"; Fletcher and Vasas, "Implementing the DMA."

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Recommends that guidelines should mandate deactivation of any design feature that poses safety or security risks to minors, such as targeted advertising and infinite scroll.

We recommend that the Commissions guidelines go further and mandate that platform design features which put minors' safety or security at risk should be disabled and never active for minors.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Requests clarification of terms like 'persuasive' design and 'real friction' in regulatory guidance.

we recommend the Commission to define 'persuasive'.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Lists features to disable for minors that could promote overuse and questions the evidence base for presuming harm in certain default settings.

Features that may contribute to excessive use, such as the number of "likes" or "reactions", communication "streaks", the " ... is typing" function, ephemeral content, and "read receipts," are turned off.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Recommends that features like AI chatbots and persuasive design components are off by default for minors and seeks an expanded definition of persuasive design.

In relation to Al chatbots integrated on online platforms, we recommend that this feature is turned off by default to reduce the potential impact for minors.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Reiterates the need for an explicit ban on manipulative design for minors under the DSA.

Explicitly ban all manipulative design including infinite scroll, autoplay, Snapstreaks, and algorithmic content loops for under-18s.

How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition). Pushes for research and threshold definitions on what constitutes digital overuse and its quality for children.

We recommend that the Commission defines thresholds for what constitutes overuse (or initiates research in this area) and explores the impact of the quality and type of attention captured.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Suggests granting platforms flexibility in healthy usage feature design based on their unique risk profiles, rather than enforcing prescriptive rules.

We encourage the Commission to clearly state that platforms should be free to design and implement screen time features in a manner consistent with their risk profile and technical design, rather than applying prescriptive expectations.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). States that guidelines should avoid outright bans on engaging features, focusing instead on making such practices safer for minors.

It is outside the scope of the Guidelines to ban or reduce access to online practices such as intermediate currencies, random rewards or products/services which seek to engage users, but rather to propose measures to ensure they are offered in a way that ensures a high level or privacy, safety and security for users who are minors.

The Case Against AI Simulated Empathy (unknown). Argues for AI design that supports offline human connection and prevents relationship risks, rather than outright bans on empathetic responses.

The solution lies in designing AI to encourage human engagement (e.g., prompting users to seek real-world connections) rather than prohibiting empathetic response

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Recommends review and potential disabling of problematic design features like autoplay and infinite scroll for minors, with stricter rules on manipulative interfaces.

Darüber hinaus wird angeregt bestimmte, besonders problematische Praktiken, wie insbesondere „autoplay", „hosting live stream" oder „endlos scrollen" daraufhin zu überprüfen, ob diese Einstellungen durch Minderjährige nicht aktiviert werden können.

Position du groupe La Poste (La Poste). Supports limiting harmful interface practices such as infinite scroll and scarcity mechanisms, especially to protect minors from risk.

S'agissant de la conception des interfaces numériques, certaines pratiques - telles que le défilement infini ou les mécanismes de rareté - sont mentionnées dans les lignes directrices comme devant être limitées, en particulier lorsqu'il existe un risque d'interaction avec des mineurs.

1.6.7 Content Moderation and Access Controls

The collected documents present a comprehensive overview of content moderation and access control strategies designed to improve child safety online within platforms and digital systems. Key measures include restricting discoverability of minor accounts, limiting contact and interaction to approved users, default-hiding or restricting profile information and engagement data, and employing always-on filtering for sensitive content in chat functions. Tiered or age-appropriate experiences, such as dedicated 'teen accounts' or the application of time-shifted streaming, are recommended to better manage risk. Further suggestions emphasize the necessity of design interventions—like purposeful friction to curb negative behaviors, prevention of automatic addition to group chats for children, and the mixing of educational with entertainment content to mitigate harmful overstimulation. Certifications from independent, state-recognized bodies and harmonization of moderation practices across platforms bolster these efforts. There is also a recurrent call for platforms to adopt trauma-informed approaches in support tools, and to ensure that youth environments are protected from unsolicited adult access, including through technical and regulatory means. The importance of safety-by-design in community standards and the proactive removal or restriction of unsuitable content and functionalities is highlighted throughout.

Ensure that minors cannot easily be found or contacted by accounts they have not previously accepted as contacts. This includes ensuring that minors' personal contact data, location data, telephone number and other content facilitating direct communication are not disclosed to accounts that the minor has not accepted as contacts. (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 (European Commission))

Accounts of minors only allow interaction such as likes, tags, comments, direct messages, reposts and mentions by accounts they have previously accepted as "friends" or contacts. This categorisation requires regular review. (TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited))

This study recommends limiting private messaging options from unconnected accounts and restricting the abilities of adult accounts to connect with child users, applying best practices and learnings from the very large social media platforms. (Salminen contribution protection of minors (Aalto University))

However, such rooms are already used in numerous cases and require protective measures. (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 Feedback (Gesellschaft für Freiheitsrechte e.V.))

Friction deliberately adds barriers to prevent antisocial behaviors on platforms. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Children reporting abuse, exploitation, or distressing content may relive trauma when describing their experience. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Raises the need to address and regulate online spaces with maximum age requirements, emphasizing the necessity for protective measures where such child-only environments exist.

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Calls for applications to intersperse calming or educational material with entertainment, preventing children from overexposure to highly stimulating content.

Apps should mix educational/calming content with entertainment to prevent flooding children with fast, flashy, high-stimulation material.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Recommends that children's follower and friend lists be hidden by default or offered as an option at registration, guarding against unnecessary sharing of relationship data.

the user's list of followers, friends or other form of connected accounts is hidden by default;

Salminen contribution protection of minors (Aalto University). Highlights the risks of private messaging for minors, proposing restrictions based on connection status and incorporating best practices from large platforms.

This study recommends limiting private messaging options from unconnected accounts and restricting the abilities of adult accounts to connect with child users, applying best practices and learnings from the very large social media platforms.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Advocates for the use of friction in user design—deliberately introducing barriers—as a moderation tool to minimize harm and the proliferation of falsehoods, especially in encrypted environments.

While most designs aim to reduce friction for engagement, purposeful friction in ethical technology design can promote reflection and minimize harm.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Argues for targeting protective measures for minors rather than imposing blanket restrictions, highlighting the effectiveness of defaulting minor accounts to private and restricting unsolicited contacts.

Instead of excessive obligations on who teens can connect with, focus in the proposed measures on measures such as those outlined above (IG Teen Accounts measures, e.g. defaulting teens into private account mode; and other more targeted measures to stop unwanted contact between adults and minors).

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Identifies the risk posed by live streams for minors and suggests time-shifted streams as a risk mitigation measure compliant with the DSA.

For this reason, time-shifted streams should be considered if possible.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Endorses youth protection programs, particularly those independently certified according to national legal requirements, as mechanisms to provide minors with high levels of privacy and security.

It should therefore be added that youth protection programs can guarantee a high level of privacy, security, and protec- tion for minors, especially if they have been tested and certified by independent experts from a self- regulatory body in accordance with criteria laid down by national law.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Explores the option of imposing conditional rather than absolute access restrictions on minors for online content, as exemplified by new legislation.

Instead of a categorical ban, lawmakers can impose conditions on minors' ability to access online content or resources.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Recommends content and functional limitations on child accounts to block risks such as grooming, profiling, and exposure to inappropriate material, with a focus on tiered user experiences.

Functionality and content restrictions can also be useful in preventing risks stemming from non-consensual contact between adults and minors (e.g. cybergrooming), algorithmic profiling and targeting, gaming (with regard to interaction risks, addiction), cost traps (e.g. loot boxes), dangerous viral challenges, and exposure to developmentally inappropriate content or advertising (e.g. harmful substances).

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Promotes trauma-informed moderation and support tools, noting that children should not be required to provide detailed descriptions of abuse to receive help.

Support tools should follow trauma-informed principles (e.g., not requiring detailed descriptions, avoiding judgemental language).

Feedback DSA (unknown). Suggests restrictions on the visibility of peer engagement, follower limits for minor accounts, and prohibition of minors having public profiles to curtail social risks.

Restrict visibility of friends' engagement (e.g., likes/comments) to reduce peer surveillance behaviors.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Mandates additional measures on video platforms for child-directed content, such as warning signals and the default deactivation of autoplay.

Das „Autoplay" für solche Inhalte sollte grundsätzlich voreingestellt deaktiviert sein.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Proposes features to prevent automatic inclusion of minors in group chats and calls for labeling and advertising restrictions for child-related content across platforms.

Mögliche Maßnahme: Kinder sollten nicht automatisch in eine Gruppe aufgenommen werden können, auch wenn sie mit der Person, die sie hinzufügen möchte, „befreundet" sind.

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 (European Commission). Sets out core principles to restrict both discoverability and the contact options of minors' accounts, together with controls on profile data exposure.

Ensure that minors cannot easily be found or contacted by accounts they have not previously accepted as contacts. This includes ensuring that minors' personal contact data, location data, telephone number and other content facilitating direct communication are not disclosed to accounts that the minor has not accepted as contacts.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Recommends clarifying the possibility and mechanisms for restricting adults from accessing child-specific online environments, mirroring age-gating for adult content.

Furthermore, we recommend clarifying, in the descriptive box in line 272, the possibility of restricting adults from youth environments in the same way that age verification aims to keep minors out of adult environments.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Details implementation of always-on filtering in chat for minors to identify and block personal data and mature language, enhancing online communication safety.

The Personal Information filter helps remove certain types of information - like email addresses and credit card numbers - from text chat conversations in real time.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Describes the enforcement of contact restrictions for minors, where only approved contacts can interact, and the setting of push notifications off by default.

Accounts of minors only allow interaction such as likes, tags, comments, direct messages, reposts and mentions by accounts they have previously accepted as "friends" or contacts. This categorisation requires regular review.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). Stresses the importance of safety by design in gaming environments and the requirement that providers adopt robust community standards along with transparent reporting and content removal processes.

Since then, PEGI Code signatories commit to implement community standards to ensure the protection of players from unsuitable content and behaviour associated with these online environments.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Notes the potential negative impact of aesthetic filters on minors' self-image, supporting their deactivation by default in social media settings.

Insbesondere Filter wie beispielsweise Beauty-Filter können die Wahrnehmung von Minderjährigen im Hinblick auf ihren eigenen Körper negativ beeinträchtigen.

1.6.8 User Empowerment and Support

This category, 'User Empowerment and Support,' centers on designing digital platforms and systems to actively support and empower children's safety and wellbeing online. Key insights emphasize the importance of proactive interventions—platforms should not merely provide passive tools, but must actively monitor for risks and respond with timely, supportive measures. Effective empowerment involves integrating easily accessible, engaging, and age-appropriate resources, such as visible help buttons, customizable time management tools, flexible reporting mechanisms, and clear onboarding experiences tailored to children's diverse backgrounds, maturity, and vulnerabilities. The documents highlight that user empowerment is best achieved through multi-layered safety strategies combining moderation, reporting, education, and support, rather than relying solely on age assurance or self-regulation tools. Inclusive design should account for children's developmental stages and offer support options ranging from digital wellness tutorials to direct helpline access. Furthermore, fostering prosocial norms—through nudging, boosting, and transparent system design—supports healthy behaviors and respectful interactions. Finally, integrating digital support with human assistance and providing user-friendly pathways for registration, account management, and parental communication are crucial to maintaining safety and building trust.

> *Proactive intervention: providers of online platforms accessible to minors should implement systems that actively monitor anonymised usage patterns to provide timely interventions to recommender systems and other user support tools that support digital wellness, rather than relying solely on reactive measures or user-initiated controls.* (Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz))

> *Reporting mechanisms must be designed to accommodate this diversity, offering flexible, inclusive options that are effective across different levels of maturity and vulnerability.* (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

> *Develop a targeted on-boarding interactive experience: once registration is complete with methods such as, e.g., tutorials, scenario-based questions ('What would you do if you land into inappropriate content?').* (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

> *LinkedIn's "Curious," "Celebrate," "Insightful," and "Support" reactions enable users to appreciate different viewpoints and express solidarity.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

> *These could also include nudges that favour safer options.* (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 (European Commission))

> *Develop a targeted on-boarding interactive experience: once registration is complete with methods such as, e.g., tutorials, scenario-based questions ('What would you do if you land into inappropriate content?').* (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Avaaz calls for unified digital wellness frameworks to prevent minors from bypassing safety measures by switching platforms and advocates for proactive monitoring and interventions to support digital wellness.

Proactive intervention: providers of online platforms accessible to minors should implement systems that actively monitor anonymised usage patterns to provide timely interventions to recommender systems and other user support tools that support digital wellness, rather than relying solely on reactive measures or user-initiated controls.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). This blueprint promotes prosocial tech design through mechanisms like signaling, nudges, and feedback systems to foster healthy behaviors; it also highlights the value of 'boosting' for building user agency.

One study found participants were more inclined to engage with opposing political views when a "Respect" button was available, compared to "Like" or "Recommend" options.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). EU Kids Online stresses the need for platform controls to be nuanced, reflecting children's diverse age, maturity, and support needs, and to cater to varying levels of disadvantage or vulnerability.

The level of control that the platform provides to minors should consider these aspects and cater for different degrees of disadvantage or vulnerability.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). INHOPE recommends a multi-layered safety approach beyond age assurance, integrating moderation, reporting, user support, and design to reduce exposure to harm.

We stress the importance of a multi-layered approach combining: moderation processes, effective reporting and redress mechanisms, user support with clear and visible routes to external help (e.g. helplines, hotlines or trusted flaggers) and design that avoids overexposure to harmful content.

Welke rol kunnen Telecom bedrijven spelen in de bescherming van kinderen in de online wereld? (KidsUnplugged). KidsUnplugged advocates for explicit, proactive government and cross-sector measures to improve online child protection.

Pleit voor grotere bescherming bij de overheid en alle sector actoren.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Missing Children Europe urges platforms to include the 116 000 missing children hotline and to design inclusive, flexible reporting mechanisms for children of varying maturity and background.

Reporting mechanisms must be designed to accommodate this diversity, offering flexible, inclusive options that are effective across different levels of maturity and vulnerability.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). The Working Group on Gaming and Regulation requests that guidelines feature more nuanced, gaming-specific examples showcasing tailored, embedded safety features and participatory design for minors.

We would welcome the addition of more nuanced, gaming-specific illustrations that demonstrate proactive risk mitigation, embedded safety features, and participatory design.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis proposes onboarding experiences and ever-present help buttons to deliver interactive and accessible safety resources to minors when they are most receptive.

Develop a targeted on-boarding interactive experience: once registration is complete with methods such as, e.g., tutorials, scenario-based questions ('What would you do if you land into inappropriate content?').

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 (European Commission). The European Commission recommends customizable, child-friendly time management tools that create real friction to reduce excessive use and incorporate nudges for safer options.

In order to be effective, these tools should create real frictions so that minors are effectively deterred from spending more time on the platform.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). KGI critiques the efficacy of digital wellbeing tools, arguing that their effectiveness, not just existence, should be demonstrated, especially since current tools are often unused by minors.

A Massachusetts legal complaint states that "TikTok ... knows such tools are ineffective because the majority of users are "unaware" of these tools, these tools are not functional or useful, and teens "lack the skills to regulate their own app usage" so these tools "remain unused by teens."

Protecting children online: response to the draft guidance (DIGITALEUROPE). DIGITALEUROPE highlights the necessity for platforms to permit default notifications from known contacts, supporting children's communication with trusted adults.

This is essential to support day-to-day communications with trusted adults such as parents or carers, and blanket restrictions on notifications could inadvertently undermine the safety and wellbeing of the child.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Save the Children calls for accessible, child-friendly registration and account deletion, using clear language and intuitive tools.

We call on the European Commission to ensure platforms facilitate child-friendly registration and account deletion processes, with accessible language and tools.

The Case Against AI Simulated Empathy (unknown). This document emphasizes that AI support tools must be thoughtfully designed and integrated with human support to address the context-dependent harms of simulated empathy.

The harms (illusion of connection, social skills gap) are real but context-dependent and addressable through thoughtful design, user education, and integration with human support systems.

1.6.9 Miscellaneous

This category gathers industry perspectives on miscellaneous platform and system design considerations for child safety regulation, with a recurring emphasis on proportionality, flexibility, and sector-specific needs. Stakeholders caution against prescriptive or excessive restrictions that could stifle innovation or undermine essential service functions, highlighting the need for adaptable guidelines that align with the objectives of the DSA without introducing unintended negative consequences. Concerns also include the recognition of standard design features—such as game randomization elements—not being inappropriately categorized as manipulative, and the importance of clarity regarding youth access to professional networking platforms, to avoid measures that would fundamentally impair their use or value to minors. Representative comments argue for allowing AI chatbots in suggested contacts when sufficient safeguards exist, for non-intrusive guidance that enables platform innovation, and for differentiated treatment of established video game design practices. There is also a call for policymakers to be explicit if their intent is to effectively bar minors from professional platforms, to avoid ambiguity and operational conflicts.

Les lignes directrices nous semblent, à ce stade, trop prescriptives. (Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM))

The use of intermittent or random rewards in video games should not be automatically classified as a manipulative design technique. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

For example, the measures would require LinkedIn to make a minor's profile invisible and inaccessible to all members with whom the minor has not proactively elected to connect on LinkedIn. (Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company))

Une prescription excessive, notamment en matière de conception de service, de paramétrage par défaut ou de fonctionnalités autorisées, pourrait freiner l'innovation et rigidifier les parcours utilisateurs. (Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM))

In other words, it would severely limit that user's ability to network and be considered for professional opportunities. (Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company))

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Meta emphasizes that measures prohibiting AI chatbots from minors' contact suggestions may be overly restrictive, arguing for the use of less excessive safeguards where possible.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). AFNUM warns against overly prescriptive guidelines for child safety, arguing such strictness can hinder adaptability, innovation, and may even degrade the online experience without guaranteeing better protection.

Les lignes directrices nous semblent, à ce stade, trop prescriptives.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). AMETIC requests that standard video game design mechanics like random rewards and randomization not be automatically classified as manipulative under the DSA, as they serve legitimate purposes in gameplay.

The use of intermittent or random rewards in video games should not be automatically classified as a manipulative design technique.

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). LinkedIn points out that proposed minor privacy measures would undermine their platform’s core function for users under 18 and asks for clearer guidance if the intent is to exclude minors.

For example, the measures would require Linkedln to make a minor's profile invisible and inaccessible to all members with whom the minor has not proactively elected to connect on Linkedin.

1.7 Parental and Guardian Controls

The central theme across Parental and Guardian Controls is the imperative to balance robust child safety with respect for minors’ rights, privacy, and dignity. Default settings and controls should be pre-installed or enabled ("activated by default on devices and online platforms frequented by minors") and designed to be both flexible and robust, allowing guardians to manage content, activity, and spending, while respecting age-related autonomy. Regulatory and legal perspectives highlight the push for harmonized, EU-wide frameworks that avoid fragmented obligations, clearly define guardianship roles, and promote industry collaboration—always ensuring tools are privacy-preserving and user-friendly. Consent and rights are central to effective controls, with calls for transparency and, where appropriate, joint consent mechanisms that prevent over-surveillance and honor diverse family arrangements. Tools should empower and support rather than restrict, fostering environments where guidance, communication, and trust between adults and minors are paramount. Usability and accessibility considerations are vital—tools must be easy to use and adapt to the needs of all guardians, including those with disabilities, and require minimal barriers to access. A dominant trend is the emphasis on cooperative safety: controls should work in tandem with platform protections and involve not only technical features but also education, practical guidance, and open communication. Across sub-categories, the overarching drive is for solutions that are effective, transparent, and equitable—protecting children without unnecessarily compromising their rights or family diversity.

1.7.1 Control Settings and Defaults

The category 'Parental and Guardian Controls >> Control Settings and Defaults' encapsulates key insights into the role of default settings and parental controls in ensuring the privacy, safety, and security of minors online. Across a variety of documents, there is a strong consensus that both device-based and account-based parental controls should be pre-installed or activated by default on devices and online platforms frequented by minors. Several contributions emphasize making such controls both flexible—so parents can adjust them as needed—and robust, with defaults set to prioritize minor safety, such as restricting risky activities or providing content filtering. Stakeholders discuss not only the technical implementation of such controls (pre-installation, opt-out defaults, age-differentiated features) but also the importance of clear information for parents and mechanisms to notify guardians if minors attempt to bypass protective settings. There is recognition of evolving autonomy

among older minors, but a recurring recommendation is for any changes to default safety settings by children to be subject to parental consent or notification. The most progressive insights extend the obligation across the entire digital ecosystem, calling for parental control functionalities to be included on all internet-connected devices sold within the EU. The debate also includes a shift towards more effective account-based solutions, given the reality of cross-device usage by minors and the advantages for parental management.

> *Enable device-based parental controls with appropriate defaults for minors for any online activity that a broad group of parents considers risky.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))
>
> *In this context, a significant aspect concerns the provision of functionalities that allow associating the minor's account with a reference parent/guardian (e.g., the email address, the account with which the parent/guardian is registered on the platform, or the phone number). In this regard, it is suggested to include this parental control measure within the default account settings (see paragraph 6.3.1 Default settings).* (AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)))
>
> *Parental control activated by default in new devices and Internet services* (EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform))
>
> *Instead of overly excessive default settings, include in the list of measures to incorporate good practices, such as focusing on essential default settings and requiring parental consent for minors under 16 to change such default settings.* (Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.))
>
> *manufacturers of Internet-enabled devices (phones, tablets, personal computers, and smart TVs) could provide detailed information to consumers concerning the risks of content not suitable for minors, as well as the available parental control options that are built into these devices.* (CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.))
>
> *In Zeile 436-438 ist aus Sicht des BMASGPK zu diskutieren, inwieweit eine autonome Umstellung der Standardvoreinstellung für Jugendliche generell oder für Kinder und Jugendliche unter einem bestimmten Alter überhaupt technisch möglich sein sollte, wenn sie sich dadurch erwiesenermaßen Risiken aussetzen würden.* (Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)))

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). This document advocates for enabling device-based parental controls with appropriate default settings for minors during online activities identified as risky by parents.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Meta recommends balanced default settings that focus on essential protections, coupled with the requirement of parental consent for minors under 16 to change such defaults, while cautioning against cumbersome restrictions.

Instead of overly excessive default settings, include in the list of measures to incorporate good practices, such as focusing on essential default settings and requiring parental consent for minors under 16 to change such default settings.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). AGCOM highlights the importance of implementing parental control mechanisms in default account settings for minors and suggests linking child accounts directly with parental accounts or contact information.

In this context, a significant aspect concerns the provision of functionalities that allow associating the minor's account with a reference parent/guardian (e.g., the email address, the account with which the parent/guardian is registered on the platform, or the phone number). In this regard, it is suggested to include this parental control measure within the default account settings (see paragraph 6.3.1 Default settings).

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). WebGroup Czech Republic calls for manufacturers to inform consumers about online risks faced by minors and to provide free, default-activated parental controls and content filtering on all new devices.

In WGCZ's opinion, it would be optimal if filtering were free and activated by default on new devices, as has demonstrably and effectively been the case with mobile devices in Great Britain for more than 15 years.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). This joint commentary supports clear and comprehensive requirements for privacy, safety, and parental controls in minors' account settings, including differentiated features and override options based on age.

The Federal Office welcomes the requirements set out in this section, which aim to protect the identity and integrity of minors.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). USK notes that default settings for minors often overlook the varying rights and competencies of older children and adolescents, suggesting settings should reflect different maturity levels.

The default settings listed in section 6.3.1 are predominantly framed from the perspective of younger children. However, there is a lack of differentiated consideration of the rights, needs, and abilities of older children and adolescents.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Additional contributors advocate that device manufacturers be required to pre-install parental controls as opt-out features, not opt-in, across the digital ecosystem.

ice manufacturers must: o Pre-install parental controls (opt-out, not opt-in)

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Echoing document 65, this additional submission calls for a mandate that device manufacturers pre-install parental controls as opt-out rather than opt-in.

ice manufacturers must: o Pre-install parental controls (opt-out, not opt-in)

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Again reinforcing prior points, the document underscores the need for universal pre-installed, opt-out parental controls on devices as a baseline standard.

ice manufacturers must: o Pre-install parental controls (opt-out, not opt-in)

EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform). The European Child Shield Platform insists upon the universal pre-activation of parental controls on both new devices and internet service contracts to protect children from harmful content.

Parental control activated by default in new devices and Internet services

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). This contribution reiterates the principle that device manufacturers should universally pre-install parental controls with opt-out as the default, reinforcing widespread support for this measure.

ice manufacturers must: o Pre-install parental controls (opt-out, not opt-in)

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). The Austrian Federal Ministry recommends that notifications be sent to parents or guardians if minors attempt to relax safety defaults, and supports automatic parental warnings in cases of excessive use.

Darüber hinaus wäre in einem solchen Fall auch eine verpflichtende Warnung/Mitteilung an die Erziehungsberechtigen hilfreich, um Kinder vor illegalen oder schädlichen Inhalten zu bewahren.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Technology Ireland supports detailed guidance for practical parental controls, advocating for flexible, EU-wide account-based systems that function efficiently across multiple devices.

We welcome the "Guidelines" for account-based parental controls, as they offer greater flexibility and effectiveness across multiple devices.

DSA Guidelines for Protection of Minors Additional Submission EuroISPA FINAL (EuroISPA). EuroISPA argues for the adoption of account-based parental controls instead of device-based ones, as these allow greater flexibility for managing minors' usage across devices remotely.

These systems provide greater flexibility and precision, enabling parents to manage settings-such as screen time, app permissions, or content filters-remotely and across multiple devices, without needing physical access.

Position du groupe La Poste (La Poste). La Poste calls for the extension of parental control features to all internet-connected devices sold in the EU, emphasizing the universality of protection across the digital landscape.

ous les appareils connectés à internet commercialisés dans l'Union européenne - notamment les ordinateurs, smartphones, tablettes, téléviseurs connectés, montres intelligentes, systèmes de navigation embarqués, consoles de jeux et liseuses - devraient intégrer une fonctionnalité de contrôle parental

1.7.2 Legal and Regulatory Compliance

The legal and regulatory compliance category for parental and guardian controls in the context of the EU Digital Services Act (DSA) centers on the need for harmonized, EU-wide frameworks for parental/guardian control systems. Many stakeholders stress the importance of establishing consistent standards to avoid fragmented national regulations, which can impede market interoperability, create legal uncertainty, and weaken child protection. Several insights advocate for frameworks that balance robust protection with privacy, innovation, and respect for minors' rights, emphasizing technical standards and industry best practices adaptable to evolving risks and technologies. Additionally, there is a strong consensus about the necessity of clearly defining terms (especially the shift from 'parental control tools' to 'tools for guardians'), supporting the diversity of caregiving roles. However, some stakeholders caution against over-reliance on parental controls as the main protective measure; instead, the onus should also be on platforms, states, and educational efforts. Parental tools should facilitate cooperative safety without compromising minors' rights or creating a false sense of security, with an overarching recommendation for privacy-preserving and user-friendly implementations.

A unified EU framework for parental control systems is crucial to prevent market fragmentation, ensure consistent child protection, and foster interoperability and innovation. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

CCIA Europe believes that a unified EU framework would help prevent fragmentation in the Single Market and ensure consistent protection for minors across platforms and services. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

an EU-level framework would: 93.1. Prevent market fragmentation: By providing a clear, consistent standard, it would avert the emergence of a complex and unworkable patchwork of differing national requirements. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

CCIA Europe recommends developing technical standards grounded in industry best practices that enable the adoption of an EU-wide interoperable framework. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

Children have a right to privacy as well as protection, which is the case also in relation to parents and other caregivers. (Overall feedback on the Commissions guidelines on measures to ensure a high level of privacy, safety and security for minors online (ECPAT Sweden))

The use of parental controls can create a false sense of safety and control as children can find ways to circumvent their parents' surveillance. (Overall feedback on the Commissions guidelines on measures to ensure a high level of privacy, safety and security for minors online (ECPAT Sweden))

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Recommends that device and app platform designers simplify and streamline parental involvement in age verification and app approvals, positioning such measures as integral to regulatory compliance for child protection.

The app store or OS can provide a simple way for parents to verify their children's ages and review and approve apps their children are using right on their phones and tablets.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Argues for a unified, EU-level approach to parental controls to prevent market fragmentation and promote consistent, interoperable, and innovative child protection mechanisms.

A unified EU framework for parental control systems is crucial to prevent market fragmentation, ensure consistent child protection, and foster interoperability and innovation.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Supports a unified parental controls framework but emphasizes the need for flexibility and adaptability to different platforms, age groups, and technological developments.

Mandating technical requirements, or prohibiting specific features displayed by online platforms, risks imposing a one-size-fits-all model that ignores the varying capacities and developmental needs of minors across age groups.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Highlights the shift toward recognizing the diverse roles of caregivers by advocating a clear, inclusive definition of 'guardians' in guidance documents.

We welcome the shift in terminology from "parental control tools" to "tools for guardians," which acknowledges the diversity of caregiving roles in children's lives.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Proposes building an EU-level, privacy-preserving, and interoperable framework for parental controls to prevent inconsistent national mandates and raise the standard of child protection.

an EU-level framework would: 93.1. Prevent market fragmentation: By providing a clear, consistent standard, it would avert the emergence of a complex and unworkable patchwork of differing national requirements.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Warns against relying solely on parental control systems for child protection, citing low adoption rates and social variability, and encourages a cooperative approach between platforms and guardians.

However, platforms should not rely on parental control systems as their primary means of protection, as we see these tools have low adoption rates and large social variability in their use.

Overall feedback on the Commissions guidelines on measures to ensure a high level of privacy, safety and security for minors online (ECPAT Sweden). Stresses the importance of education and platform-level measures over mere reliance on parental controls, noting that controls may give a false sense of security and minors have privacy rights.

The use of parental controls can create a false sense of safety and control as children can find ways to circumvent their parents' surveillance.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Advocates the establishment of an EU-wide framework for parental controls to ensure cohesive child protection and foster technological innovation.

The Commission could consider creating a unified EU framework for parental control systems to help prevent market fragmentation, ensure consistent child protection, and foster interoperability and innovation.

DSA Guidelines for Protection of Minors Additional Submission EuroISPA FINAL (EuroISPA). Calls for the EU to harmonize parental control tools to encourage privacy-preserving, user-friendly solutions and avoid regulatory fragmentation.

Establishing a harmonised EU framework for parental control systems is essential to avoid market fragmentation, ensure consistent levels of child protection across Member States, and promote interoperability and innovation.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). Urges recognition and certification of parental control tools by regulatory bodies, suggesting that such certified tools influence age classification of digital content.

The existence of certified parental control tools must be taken into account during the examination process when classifying games for a particular age group and may have a positive impact on the classification of the video game.

DSA (Protection of Minors) Guidelines (Samsung Electronics). Supports an EU-wide framework for parental controls to prevent conflicting obligations from divergent national laws and maintain consistency beyond online platforms.

While these Guidelines are not suitable to solve this issue as their scope is limited to online platforms, SE continues to support an EU-wide framework for parental control and minor protection to avoid continued fragmentation and conflicting obligations for companies operating across EU Member State borders.

1.7.3 Consent and Rights Management

The "Consent and Rights Management" category explores the complexities and safeguards necessary when implementing parental or guardian controls for minors' online experiences, particularly under the context of the EU Digital Services Act. Several key themes emerge: the need for clear, transparent notification and safeguards for minors when guardians activate monitoring features (especially to prevent misuse or over-surveillance); the importance of respecting children's privacy, autonomy, and rights—even as parental controls are deployed; and the critical question of how and when minors' consent should be required, sometimes advocating for 'double-consent' systems. Documents also highlight operational and conceptual challenges, such as verifying true parental authority and managing non-traditional family structures, which can inadvertently exclude or endanger vulnerable minors. Guidelines are urged to balance protective intent with careful attention to not disproportionally restrict minors' access to important resources, especially for marginalized groups. Mechanisms for independent recourse, transparency regarding monitoring, and making parental controls optional rather than mandatory are recurrent recommendations. Ultimately, rights-respecting, age-appropriate, and transparent consent procedures are emphasized, especially for high-risk actions and across diverse family situations.

Provide clear a notification to minors of their activation by guardians and put other safeguards in place considering their potential misuse by guardians such as, for example, providing a clear sign to the minor in real time when any monitoring functionality is activated and transparent information of

what is being monitored and the specific settings that can be changed by the caregiver or guardian. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

We therefore recommend that the Guidelines should specify that tools for guardians should "not disproportionately restrict minors' rights to privacy, to freedom of information and freedom of expression or to access services." (SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International))

We would encourage the Commission to clarify this point and to support a consent-based approach for all parental control tools. (Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office))

regulators are routinely creating parental consent requirements for minors' access to online content or resources. These requirements act like conditional access restrictions, i.e., minors can access the resources, but only after the publisher and minor obtain parental consent. (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Any parental controls introduced must respect privacy, transparency, and consent. (Protecting children online: response to the draft guidance (DIGITALEUROPE))

any parental consent requirement must anticipate that some parents will act otherwise. (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

As the Irish Data Protection Commission has said, "there aren't yet many ways of checking parental consent which are accurate, proportionate and that actually work in practice." (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Requiring tools for guardians such as screen time controls, guardian oversight over minor account settings, and total visibility into minor communications/interactions with other accounts may be problematic, disproportionate, and potentially in violation of the rights of the minor. (Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild advocates for clear, real-time notifications to minors regarding supervisory features, transparent information about what is monitored, and age-appropriate empowerment of minors, including requiring their consent for monitoring as they mature.

Provide clear a notification to minors of their activation by guardians and put other safeguards in place considering their potential misuse by guardians such as, for example, providing a clear sign to the minor in real time when any monitoring functionality is activated and transparent information of what is being monitored and the specific settings that can be changed by the caregiver or guardian.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Amnesty International stresses that parental control tools should not unduly restrict minors' rights to privacy, freedom of information, and expression, nor impede access to essential online services.

We therefore recommend that the Guidelines should specify that tools for guardians should "not disproportionately restrict minors' rights to privacy, to freedom of information and freedom of expression or to access services."

Guidelines on the protection of minors feedback CTU (Czech Telecommunication Office). The Czech Telecommunication Office highlights the importance of a consent-based approach to parental controls, clarifying when minors' consent is necessary and proposing options like 'double-consent' and involving guardians in registration processes.

We would encourage the Commission to clarify this point and to support a consent-based approach for all parental control tools.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). This document critiques the assumed benefits of parental consent requirements, highlighting the risks of abuse, exclusion of vulnerable minors, operational challenges in verifying parental status, and the potential for such controls to erode children's rights and access.

regulators are routinely creating parental consent requirements for minors' access to online content or resources. These requirements act like conditional access restrictions, i.e., minors can access the resources, but only after the publisher and minor obtain parental consent.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis recommends making verified adult support optional for high-risk settings (e.g., live streaming), particularly for younger children, without making blanket parental involvement compulsory.

The proposed guidelines also lack requirements for parental involvement in certain high-risk changes. In cases involving enabling live streaming, sharing geolocation, or facilitating interactions with strangers, some form of verified adult consent could be warranted, particularly for children under 13.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Middle Tech Europe calls for parental controls to be optional and not infringe upon children's rights, underscoring the need for alternative safety strategies that respect the autonomy and privacy of minors.

e advocate strongly for a pragmatic approach on the basis that minors can be kept safe without providing "active monitoring tools" for parents (e.g., with age assurance where access to mature content is concerned) and that they may have legitimate reasons for seeking information or community without parental knowledge - for example, in cases where they may be in an abusive home situation.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Epic Games describes implementing 'Cabined Accounts' where younger players can access games but require parental consent for certain features, showing a granular, age-based approach to consent management in gaming.

Players with Cabined Accounts can still play Epic games but cannot access certain features until their parent or guardian provides consen

Protecting children online: response to the draft guidance (DIGITALEUROPE). DIGITALEUROPE supports parental controls that complement, rather than override, children's rights and privacy, advocating for transparency, age-appropriate safeguards, and respect for both child autonomy and family choice.

Any parental controls introduced must respect privacy, transparency, and consent.

DSA Guidelines for Protection of Minors Additional Submission EuroISPA FINAL (EuroISPA). EuroISPA highlights the need for independent safeguards and complaint mechanisms to protect minors from misuse of guardian tools, such as excessive surveillance or restricting access to support.

Mechanisms for independent review, complaints, or escalation in cases of misuse would better protect minors' rights.

1.7.4 Parental Guidance and Support

The key knowledge in the category of Parental Guidance and Support emphasizes that parental and guardian control tools should empower and support children in navigating online spaces safely, rather than acting solely as restrictive measures. Multiple documents stress the importance of these tools working as complementary measures alongside built-in platform protections, not as standalone solutions, to provide a high standard of privacy, safety, and security for minors. There is broad advocacy for device-level controls, flexibility in tool design according to age and developmental needs, and attention to proportionality in considering existing safeguards. Moreover, effective parental support extends beyond technical controls, encouraging platforms to equip guardians with clear guidance, accessible resources, and direct links to support services tailored to varying digital literacy levels. Involving children and families in the co-design of features and offering easy avenues for trusted adult involvement represent progressive strategies to foster both agency and protection. The crucial balance is to maximize safety while upholding children’s rights to privacy and access, and to promote supportive environments both digitally and within families.

The Guidelines specify that tools for guardians should only be considered supplementary to safety-by-design and default measures, as well as any other measures implemented to comply with Article 28(1)

of the DSA. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

In respect of children's rights and agency, language should be amended to encourage parental controls that mostly empower children by supporting them to navigate online platforms safely, rather than managing their experience on their behalf. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

We stress that guardians also need appropriate and understandable resources and to be redirected to support services. (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))

Guardians should be redirected to relevant support services to ensure they are not left alone in managing complex risks. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

WGCZ has thoroughly demonstrated that all existing Website-Level AV tools are inadequate to protect minors, particularly given the vast and diverse nature of the online environment. (CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.))

Mandatory parental control on the device, meaning having by default a proof that a user has the age of majority or not, would make it possible to block (i) the consumption of adult content at large, but also (ii) to block other types of harmful content for minors such as conspiracy videos, violence, misinformation, and nevertheless (iii) to limit exposure to unsuitable advertising or websites and mobile applications (e.g. gambling). (Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Highlights the need for parental controls that empower children to navigate platforms safely, prioritizing children's agency over restrictive parental management.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). Emphasizes the complementary role of parental supervision tools provided by device manufacturers and OS developers, recognizing that they supplement but should not replace platform-level protections.

Les systèmes de contrôle parental et plus largement de supervision des terminaux par les parents (contrôle du temps d'écran ou de téléchargement des applications), viennent utilement en complément des outils de protection mis en place par les plateformes, mais sans s'y substituer.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Clarifies that guardian tools should supplement, not replace, safety-by-design and default protective measures as per regulatory requirements.

The Guidelines specify that tools for guardians should only be considered supplementary to safety-by-design and default measures, as well as any other measures implemented to comply with Article 28(1) of the DSA.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Reiterates that parental controls are to be seen as complementary to core safety techniques, and can enhance safety if used alongside other protective measures.

The Guidelines state that tools for guardians should only be treated as complementary to the safety by design and default measures and to any other measures put in place to comply with Article 28(1) DSA.

DOT Europe response1 (DOT Europe). Suggests that the appropriateness and necessity of parental controls should be assessed in the context of existing age assurance mechanisms on platforms for proportionality.

However, we underline that parental controls may not be appropriate nor proportionate for certain online platforms which have, for instance, already put in place robust age assurance mechanisms.

CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.). Argues that device-level parental controls are optimal for minor protection, as opposed to inadequate website-level measures, emphasizing the primacy of guardian tools.

Filtering and Parental Control at Device-Level are Optimal Tools to Protect Minors While Minimising Security Risk and Violation of Individual Freedoms and Privacy Rights;

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Recommends default device-level parental controls to block a wide range of harmful content, urging the Commission to work with OS and hardware providers for implementation.

We therefore encourage the Commission to consider recommending device-level parental control mechanisms as part of the broader protection framework for minors, and to collaborate with OS providers and hardware manufacturers to promote default configurations that empower parents while respecting children's rights.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Calls for platforms to equip guardians with resources, practical tools, and support services to better guide children online, catering these to different family needs.

This includes providing clear, accessible resources on online grooming risks, including those arising from peer interactions or manipulative relationships, as well as practical support such as: conversation starters to help families discuss online safety; direct access to helplines and child protection services; visual or plain-language guidance tailored to varying levels of digital literacy and socioeconomic context.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Encourages platforms to introduce features that facilitate support from trusted adults, recognizing that many children may reach out to known adults rather than formal reporting mechanisms.

Some children are more likely to seek help from a known adult rather than a faceless report mechanism.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Advocates for broader family support by encouraging platforms to co-design features with families and children, and to support digital literacy and digital parenting programs.

These include, but are not limited to, co-designing different tools and features with children and their guardians, providing funding for schools or family organisations to boost digital literacy and digital parenting programmes, structural measures in their own HR to build family-supportive workplaces.

Microsoft response to the European Commission's draft 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 (Microsoft). Underscores that family safety tools are an important part of the risk mitigation suite, but should not be the sole reliance for minors' online protection.

As outlined in the draft Guidelines, tools for guardians should not be treated as the sole mitigation measure to address risks to minors on an online platform.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Calls for urgent expert and parental involvement in formulating recommendations concerning children's use of social media, prioritizing the precautionary principle.

Hierbij experten en praktijkdeskundigen uit te nodigen die verschillende stemmen laten horen, wetende dat het voorzorgsprincipe allerbelangrijkst is in de bescherming van kinderen.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Emphasizes the requirement for platforms to provide guardians with understandable resources and direct them toward appropriate support services.

We stress that guardians also need appropriate and understandable resources and to be redirected to support services.

Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation). Supports guardian controls that are easy to use and child-centered, stressing they should enable evolving capacities and not overly restrict children's privacy or access.

We also support the requirement for guardian control tools that are easy to use and not disproportionately restricting children's rights to privacy or access to services.

1.7.5 Transparency and Communication

The insights gathered across these documents emphasize that effective parental and guardian controls should be rooted in transparency, open communication, and mutual trust with minors. Rather than relying solely on restrictive measures or covert monitoring, experts advocate for age-appropriate, honest information about monitoring activities, their purposes, and their impact on children's well-being. Dialogue, empowerment, and joint understanding between guardians and children are seen as key to safety. Several contributions underscore the need for mechanisms that make children aware of monitoring functionalities, whether through real-time or status notifications, to promote responsible behavior and reduce secrecy. There is also support for tools and prompts that encourage children to involve parents or trusted adults in decisions with potential risks. Moreover, the importance of clear, accessible messaging from authorities and platforms about parental controls, age limits, and online risks is highlighted, both for empowering guardians and ensuring children's welfare.

Communication: Parents should engage in open and curious conversations about their children's online lives. (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))

Children deserve age-appropriate information about any monitoring taking place (what is being observed, why it matters and how it contributes to their well-being) to avoid fostering fear or secrecy. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

To provide children with visibility and understanding of the controls their parents have enabled, Epic informs children when their guardians enable Time Limits or Time Reports. (Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games))

The proposed guidelines describe "real time" notification to a minor user that a monitoring function has been activated by an authorized guardian (line 858). (Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children))

Such notifications may introduce increased vulnerability and incentivize secrecy by allowing minor users to feel free to engage in inappropriate or risky conduct when monitoring is inactive, knowing that they could quickly change behavior (disconnecting from a particular gaming server, ending a chat, deleting shared images, etc.) upon receiving a "real time" notification that monitoring functionality is activated. (Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children))

Children see in-game notifications when they have 30 minutes left in Fortnite and UEFN. (Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games))

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Advocates for shifting parental involvement from enforcing control to fostering open, curious conversations about children's online experiences, underpinned by trust and interest.

Communication: Parents should engage in open and curious conversations about their children's online lives.

Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (National Center for Missing & Exploited Children). Recommends an always-on notification about monitoring, rather than real-time alerts, to reduce risky behavior and secrecy among minors while supporting transparency.

Instead, consider suggesting a notification scheme that indicates only whether such monitoring functionality has been enabled on a minor's account.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Suggests integrating prompts within services that encourage children to seek parental or trusted adult guidance when facing high-risk online decisions, thus strengthening transparency and protection.

In addition to the existing transparency recommendations, we suggest including prompts that actively encourage children to involve a parent or trusted adult before making decisions or taking actions that could pose a high risk to the

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Highlights the need for trust, dialogue, and clear, age-appropriate information in digital safety tools, so children feel informed rather than fearful about online monitoring.

Children deserve age-appropriate information about any monitoring taking place (what is being observed, why it matters and how it contributes to their well-being) to avoid fostering fear or secrecy.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Supports real-time notifications to minors regarding active guardian surveillance, to prevent misuse and uphold transparency in monitoring practices.

We support measures designed to protect children from potential misuse of monitoring capabilities by guardians, particularly the implementation of real-time notifications that clearly inform minors when any surveillance functionality is active.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Describes concrete measures for transparency, such as notifying children when parents enable controls or set time limits, and allowing requests for extended access.

To provide children with visibility and understanding of the controls their parents have enabled, Epic informs children when their guardians enable Time Limits or Time Reports.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Calls for stronger, clearer messaging to parents about online risks, the impact of problematic situations, and age limits to better empower guardians and protect children.

Ze moet de leeftijdsbeperkingen duidelijk en regelmatig communiceren, gezien die vandaag nauwelijks bekend zijn en erg vaak omzeild worden, vaak ook door ouders zelf omdat ze niet bewust worden gemaakt van de potentiële gevaren.

1.7.6 Content, Activity, and Spending Controls

The insights across these documents emphasize the need for comprehensive, user-friendly, and effective parental and guardian controls over content, activity, and spending for minors online. These controls should empower parents and guardians to manage what content minors can access, monitor and regulate online activity (such as social interactions and screen time), and prevent unwanted purchases, all while respecting data

minimization principles. There is a consistent call for tools that are transparent, accessible, and adaptable to the needs of both children and parents, including mechanisms that notify parents if their child encounters inappropriate content or attempts to spend money online. Several documents highlight the importance of balancing parental controls with platform responsibility and usability—recognizing that many parents may be overwhelmed by technology. Recommendations also include providing comprehensive education and reporting tools, involving child development specialists in design, and considering both industry standards and regulatory alignment. Notably, the debate also involves whether the emphasis should be on age assurance or a broader toolkit of parental controls—favoring the latter to ensure both privacy and safety. Finally, specific suggestions are raised to clarify policy language (for example, regarding prevention of unwanted purchases) and to encourage collaboration among industry stakeholders to set standards that address pain points experienced by families.

> *Art 28b(3) (h) providing for parental control systems that are under the control of the end- user with respect to content which may impair the physical, mental or moral development of minors* (Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services))
>
> *the section on tools for guardians reiterates that effective control mechanisms must allow caregivers to manage not only time and spending but also the nature and type of content accessible to minors.* (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))
>
> *These controls let parents and guardians manage access to social features such as voice and text chat, purchasing permissions, and more.* (Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games))
>
> *Clarify what "easy to use, age-appropriate" guardian control tools are.* (Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services))
>
> *Ensure that minors are not exposed to unwanted purchases, e.g. by considering deploying effective tools for guardians (see Section 7.3 on Tools for guardians).* (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 (European Commission))
>
> *a dashboard gives a daily breakdown and indicates when a parent or guardian has granted extra time for their child.* (Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Advocates for a reporting mechanism enabling minors to directly notify parents about non-age-appropriate content, supporting parental involvement in handling content issues.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Recommends transparent safety controls and default parental settings for risky online activities to enhance user and child safety.

Enable device-based parental controls with appropriate defaults for minors for any online activity that a broad group of parents considers risky.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Supports parental control systems granting end-users authority over content access, emphasizing their complementarity to existing safety and regulatory measures.

Art 28b(3) (h) providing for parental control systems that are under the control of the end- user with respect to content which may impair the physical, mental or moral development of minors

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Critiques the overemphasis on age assurance, suggesting a wider range of proportionate parental controls while considering data minimization.

Disproportionate focus on age assurance: Age assurance measures remain the focus of the guidelines, even though, according to the basic understanding, other measures should also be considered as proportionate solutions.

Welke rol kunnen Telecom bedrijven spelen in de bescherming van kinderen in de online wereld? (KidsUnplugged). Calls for industry-wide standards and assessment of existing parental control options, with focus on addressing parental challenges in setup and use.

In kaart brengen van ouderlijke toezicht opties die vandaag worden aangeboden aan ouders; wat zijn de specifieke pijnpunten die ouders ervaren bij het instellen van controles?

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Stresses the importance of providing minors with accessible tools to manage and limit their screen time on digital platforms.

a covered platform shall provide a user that the covered platform knows is a minor with a readily accessible and easy-to-use option to limit the amount of time spent by the minor on the covered platform.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Showcases industry examples like Screen Time and Communication Safety, and commits to developing further tools for parental monitoring and child protection.

Apple is proud of our industry-leading innovations, including Screen Time and Communication Safety, that help keep children safe on our devices while honoring our commitments to the other rights of our users.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Advocates for stronger and evaluable parental control tools, noting the necessity of platform responsibility when parents face digital literacy challenges.

Da jedoch Eltern in der digitalen Welt oftmals selbst überfordert sind, ist unabhängig von funktionierenden Tools für Erziehungsberechtigte die Plattformverantwortung essentiell.

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 (European Commission). Recommends deploying tools that allow guardians to prevent minors from making unwanted online purchases.

Ensure that minors are not exposed to unwanted purchases, e.g. by considering deploying effective tools for guardians (see Section 7.3 on Tools for guardians).

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Argues for child-friendly, inclusive parental controls designed with input from child development specialists, and for comprehensive management across time, spending, and content.

Tools must be presented in a child-friendly, inclusive manner, and guidelines must incorporate insights from child development specialists.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Reiterates the necessity for end-user-controlled parental systems to protect minors from content that could negatively impact their development.

Art 28b(3) (h) providing for parental control systems that are under the control of the end- user with respect to content which may impair the physical, mental or moral development of minors

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Details robust parental controls that allow guardians to manage minors' playtime, access, and social interactions across digital platforms.

These controls let parents and guardians manage access to social features such as voice and text chat, purchasing permissions, and more.

Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency). Requests clarification regarding recommendations on unwanted purchases by minors and queries the legal interpretation surrounding such exposures.

It is unclear what the recommendation to ensure that minors are not exposed to unwanted purchases means.

1.7.7 Usability and Accessibility

The insights under the category 'Parental and Guardian Controls >> Usability and Accessibility' converge on the need for parental control tools to be user-friendly, accessible, and adaptable to diverse guardian and child needs. There is strong emphasis on making these tools easy to use, particularly for guardians with disabilities or additional accessibility needs, and ensuring that accessing such tools does not require mandatory registration or account creation. Flexibility and non-intrusiveness are highlighted, advocating for tools that allow informed, proportionate choices tailored to individual children. The documents further recognize the importance of integrating digital literacy initiatives to maximize tool effectiveness, and call for practical guidance for how platforms can implement these measures, including in complex usage scenarios like cross-device or third-party control environments.

It is therefore essential not only that guardians have the right tools to exercise this role, but that these tools are easy to use and accessible. (Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple))

Monitoring tools should be flexible and adaptive rather than intrusive. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

COFACE suggests adding (line 850-863) that these tools should be accessible to all guardians, including guardians with disabilities or additional accessibility needs. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

Monitoring tools should be flexible and adaptive rather than intrusive. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

reference should also be made to Article 47 of the DSA and to the EU Accessibility Act. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

Encouraging awareness and digital literacy will also play a part in ensuring the effectiveness of these tools. (Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple))

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Advocates for providing accessible, easy-to-use guardian tools and stresses the importance of promoting digital literacy and awareness to enhance child protection online.

It is therefore essential not only that guardians have the right tools to exercise this role, but that these tools are easy to use and accessible.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Emphasizes the need for flexible, non-intrusive monitoring tools that support proportionate choices and do not mandate guardian registration or account creation.

Monitoring tools should be flexible and adaptive rather than intrusive.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Highlights that parental control tools must be accessible to guardians with disabilities or additional needs, in line with EU standards, and available without requiring an account.

COFACE suggests adding (line 850-863) that these tools should be accessible to all guardians, including guardians with disabilities or additional accessibility needs.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Stresses the need for parental control tools that are simple and easy to use for all guardians.

outils de contrôle parental faciles d'utilisation

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Restates the call for easy-to-use, accessible guardian tools, reinforced by digital literacy initiatives to maximize their efficacy and child protection impact.

It is therefore essential not only that guardians have the right tools to exercise this role, but that these tools are easy to use and accessible.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Requests further clarification to help platforms implement usability and accessibility requirements, especially for cross-device and third-party control scenarios.

We recommend adding further clarification on how platforms can meet these goals in practice, particularly in cross-device environments or where third-party controls are used.

1.7.8 Miscellaneous

1.8 Recommender Systems and Personalization

The most compelling insight across these sub-categories is a concerted move away from recommender systems that prioritize engagement or behavioral profiling for minors, shifting instead toward safeguarding children's rights, developmental needs, and wellbeing. Many documents stress that systems should centre on explicit, user-provided preferences and robust privacy protections: "explicit, user-provided signals such as declared interests or preferences are widely favored over implicit, engagement-based data collection." There is universal support for increased user control and transparency, advocating for child-friendly interfaces where minors can reset or opt out of personalization, alongside clear, age-appropriate explanations for recommendations. Several categories highlight the demand for governance and measurement innovations—including transparency, standard-setting, periodic impact assessments involving children, and targeted, risk-proportionate responses that acknowledge platform and context specificity. A strong thread concerns minimizing profiling and behavioral tracking, with contextual or non-personalized experiences encouraged as the baseline, especially for sensitive or high-risk content. Categories relating to content quality emphasize actively promoting diversity, factual accuracy, and civil discourse, balancing minors' agency and interests with content from trusted or prosocial sources. Overall, the field is trending toward contextualized, accountable, and customizable recommender systems that respect children's evolving capacities and prioritize wellbeing over engagement. Common elements include transparency, user empowerment, risk-awareness, and a pressing need to balance safety and privacy with the positive potential of personalization.

1.8.1 Algorithmic Design and System Objectives

The collected insights from the documents converge on the need for a paradigm shift in the objectives and design of recommender systems, particularly when serving minors. A strong consensus emerges against optimizing for engagement metrics (such as time spent or interaction), which can potentially result in addictive behaviors or the amplification of harmful content. Instead, these insights champion the prioritization of minors' best interests, emphasizing the importance of considering their specific needs, characteristics, accessibility requirements, and rights. The documents argue for the incorporation of alternative metrics such as accuracy, diversity, inclusivity, fairness, relevance, credibility, and safety into recommender system objectives. Some emphasize the necessity for platforms to adopt explicit user-provided signals and feedback rather than relying

solely on implicit engagement indicators. Additionally, there is advocacy for technical and governance innovations: ideas include replacing engagement-oriented metrics with user-perceived quality, prioritizing content from trusted actors, and even utilizing depolarization scores to bridge ideological divides. Calls are made for transparency and the establishment of standards, noting current gaps in qualitative and quantitative assessment metrics. Overall, the recommendations seek to ensure algorithms foster a safer, more inclusive, and prosocial online environment for minors, supporting their development and well-being over the commercial incentive of maximizing engagement.

> *Take into account specific needs, characteristics, disabilities and additional accessibility needs of minors and their rights when defining the objectives, parameters and evaluation strategies of recommender systems, in particular by not only optimising or predominantly maximising time spent on, engagement and interaction with the platform.* (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))
>
> *e recommend amending the wording to: ""[to take into account specific needs, characteristics, disabilities and additional accessibility needs of minors when defining the objectives, parameters and evaluation strategies of recommender systems, parameters and metrics related to accuracy, diversity, inclusivity and fairness should be prioritized over engagement and interaction with the platform."* (SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International))
>
> *Parameters and metrics related to accuracy, diversity, inclusivity and fairness should also be considered.* (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 (European Commission))
>
> *Replace engagement optimizations (e.g., view time, comments, shares, more ad distribution) with optimizations for user-perceived quality, especially on sensitive topics.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))
>
> *Personalisation has been a promise made by social media platforms to their users.* (Safe by Default (Panoptykon Foundation))
>
> *To ensure that all recommender systems that also optimize for engagement metrics are captured, we recommend removing "only" in line 529.* (Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates designing recommender systems for minors by considering their specific needs and rights, not just engagement optimization.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Calls for prioritizing metrics such as accuracy, diversity, inclusivity, and fairness over engagement in recommender systems for minors.

> *e recommend amending the wording to: ""[to take into account specific needs, characteristics, disabilities and additional accessibility needs of minors when defining the objectives, parameters and evaluation strategies of recommender systems, parameters and metrics related to accuracy, diversity, inclusivity and fairness should be prioritized over engagement and interaction with the platform."*

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Suggests moving away from engagement optimization to user-perceived quality and amplifying trusted voices on sensitive issues.

> *Prioritize public amplification to actors that varied users explicitly know and trust.*

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Proposes the use of metrics beyond engagement, including user satisfaction and intergroup communication, to evaluate recommender systems.

> *Use indicators such as user-reported satisfaction and intergroup communication*

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Recommends that recommender prompts for minors are intentionally designed to reduce addictive tendencies and 'rabbit hole' effects.

This is a key element to help minors get out of so-called 'rabbit holes', also mentioned in footnote 41 of the guidelines.

Safe by Default (Panoptykon Foundation). Argues against engagement-based optimization and proposes prioritizing relevance, credibility, and safety to achieve true personalization.

We argue that as long as algorithmic content curation is optimised for user engagement (being an overarching commercial objective), the outcome (recommended content) is not 'personalised', only 'targeted".

Feedback DSA (unknown). Recommends chronological feeds over algorithmic ones for minors to decrease risk of manipulation and dependency.

Prioritize chronological feeds for minors over algorithmically curated ones to reduce emotional manipulation and dependency.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Calls for explicit training of recommender systems to avoid surfacing abuse material and related advertisements.

Recommender systems should be explicitly trained/optimized to avoid surfacing abuse material, including advertisements for services promoting access to abuse material

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Critiques current guidelines for lacking concrete algorithmic requirements to prevent excessive and addictive use among minors.

Es wird lediglich gefordert, dass Empfehlungssysteme „nicht zu exzessiver Nutzung“ führen sollen, jedoch werden keine Anforderungen an Algorithmen gestellt, die potenziell süchtig machende Inhalte (z. B. schnelle Belohnung, extreme Inhalte) bevorzugen.

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 (European Commission). Recommends adapting recommender systems for minors by prioritizing explicit user signals and a range of inclusive metrics.

Prioritise 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Advocates capturing all recommender systems that optimize for engagement metrics by adjusting the wording in guidelines.

To ensure that all recommender systems that also optimize for engagement metrics are captured, we recommend removing "only" in line 529.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Recognizes the need to consider accuracy, diversity, inclusivity, and fairness, but notes current absence of agreed assessment methods.

The draft guidelines also discourage reliance on engagement-based signals for content delivery to minors, referring to "parameters and metrics related to accuracy, diversity, inclusivity and fairness [that] should also be considered."

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Suggests greater clarity in

guidelines regarding optimization objectives, highlighting that few systems optimize solely for engagement.

For clarity, we would recommend that the guidelines be more precise in describing optimization. Few platform recommender systems would optimize only for engagement. Rather, many recommender systems are designed to include a ranking step that incorporates other signals about content diversity.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Asserts that recommender system objectives and parameters should always center the best interests of the child, not engagement.

We suggest clearer emphasis in the guidelines as to the fact that objectives, parameters and strategies for recommender systems should always put the best interests of the child at the centre, instead of maximising engagement.

Consultation Response from Barnevakten, Norway - Regarding Article 28 of the EU Commission's Digital Services Act (DSA) (Barnevakten Foundation). Supports adapting algorithms to explicit user feedback rather than relying only on observed user behavior.

We support the proposal that platforms must adapt more to users' explicit feedback about the algorithms, and not rely solely on user behavior (line 539-).

1.8.2 Profiling, Data Use, and Default Settings

The documents reflect a strong consensus on protecting minors from intrusive profiling and behavioral tracking in online recommender systems. A recurring recommendation is to set non-user profiling (i.e., non-personalized or contextual) recommender systems as the default for children, ensuring these options are both effective and child-friendly. Explicit, user-provided signals such as declared interests or preferences are widely favored over implicit, engagement-based data collection (like watch time or clicks) for content recommendations aimed at minors. Several stakeholders advocate for minors' autonomy in resetting or tailoring their feeds, combined with transparency in how recommendations are generated. Safeguards like prohibiting the use of behavioral data collected outside the platform, avoiding manipulative or addictive recommendation loops, and offering clear benchmarks or oversight for these systems are also emphasized. A few documents discuss the challenge of balancing privacy with maintaining service quality, with concerns raised regarding blanket bans on all behavioral data which may impede safer, tailored user experiences. Overall, the prevailing view is that recommender systems for minors should minimize profiling, use explicit signals as default, and include robust data protection, transparency, and child-friendly design principles.

Protect children from harmful or addictive content loops by setting non-profiling mode as the default for all child users. (SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands))

the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly. (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation))

Prioritise Use 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors, unless the minor indicates otherwise by changing their settings. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Homo Digitalis expresses significant reservations regarding the proposed blanket prohibition outlined in measure 535-8, which restricts the use of "ongoing behavioural data" in recommender systems serving minors. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

However, the recommender system could easily be rebuilt if the underlying datasets and interest profiles are not also deleted or detached from the recommender system. (The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority))

l'Arcom note que le projet de lignes directrices encourage les plateformes à « donner la priorité aux "signaux explicites fournis par l'utilisateur" plutôt qu'aux "signaux implicites basés sur l'engagement" afin de déterminer le contenu affiché et recommandé aux mineurs ». (Contribution de l'Arcom à la

consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom))

Urgent Concerns Regarding Online Marketing to Children on Digital Streaming Platforms and the Adequacy of Current Regulations (Inria). Calls for DSA guidelines to explicitly prohibit offering minors recommender systems based on profiling when ads are also profiling-based, emphasizing alignment with Article 28.1.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates prioritizing explicit user-provided signals over implicit engagement metrics in content recommendations for minors, unless settings are deliberately changed by the minor.

Prioritise Use 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors, unless the minor indicates otherwise by changing their settings.

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). Supports the ability for minors to reset their recommender systems, stressing the need to fully delete associated profiles and data to genuinely reset feeds.

However, the recommender system could easily be rebuilt if the underlying datasets and interest profiles are not also deleted or detached from the recommender system.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Recommends permanently halting behavioral tracking of children for content recommendation and stopping the collection of sensitive personal data for personalization.

Whilst these risks are not unique to child users, we believe that a permanent halt to behavioural tracking of children for the purposes of content recommendation on social media platforms is a critical step towards a safer online environment for children.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Suggests introducing clear benchmarks and external oversight for age assurance and recommender systems to better protect minors.

a) Age assurance: for this tiered approach to be effective, the terms "high risk" and "medium risk" must be defined with clear benchmarks. Additionally, the assessment should be subject to external oversight, avoiding self-assessment by companies. The potential for age assurance to also complement age appropriate design should be clearly recognised.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Urges clarification that recommender systems using explicit signals should not be considered 'profiling' under the DSA for minors and points to examples of safer recommendation approaches.

For example, the Better Feeds report published by KGI suggests ways to develop recommender systems that are optimised for long-term user value, using - amongst other things - explicit user signals.

Safe by Default (Panoptykon Foundation). Recommends prohibiting default interaction-based recommendation systems to protect consumers under the DSA, referencing alternative feed options.

The European Commission must follow Ireland's lead, and switch off Big Tech's toxic algorithms",

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Calls for non-user profiling recommender systems to be the default option for children, with child-friendly design retained.

the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Advocates for recommendation systems for minors to avoid implicit behavioral profiling, relying instead on explicit user signals and filtering harmful content.

Recommendation systems must avoid implicit behavioural profiling.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Emphasizes setting a non-profiling mode by default in recommender systems for children to prevent harmful or addictive content loops, with transparency in system operation.

Protect children from harmful or addictive content loops by setting non-profiling mode as the default for all child users.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Recommends making non-user profiling recommender systems the default for children, ensuring these remain user-friendly.

d) Recommender systems and moderation: the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

STATEMENT (Digipeace (Digirauha ry)). Advocates for default non-user profiling in recommender systems for minors, ensuring usability and safety.

d) Recommender systems and moderation: the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Raises concerns about overly restrictive bans on behavioral data in recommender systems, cautioning that it could undermine basic operational capacity.

This provision, as currently drafted, may fundamentally undermine the basic operational capacity of recommender systems.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Reiterates the recommendation for defaulting to non-user profiling recommender systems for child users with child-friendly characteristics.

the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Endorses making non-user profiling recommender systems the standard default for children, focusing on child-friendliness.

the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

Feedback DSA (unknown). Proposes that recommender systems for minors should not utilize behavioral data from outside the relevant platform.

Recommender systems for minors should not rely on behavioral data gathered outside the platform (e.g., from other apps (even though from the same company) or device-level tracking).

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Suggests platforms should by default disable the use of engagement-based implicit signals for minors and prioritize explicit user signals.

L'Arcom suggère d'ajouter dans les lignes directrices la recommandation pour les plateformes de désactiver par défaut l'utilisation de signaux implicites basés sur l'engagement

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Supports making non-profiled recommender systems the default for minors, with design that avoids behavioral inference or engagement maximization.

Non-profiled recommender systems should be the default setting for minors, with design principles that do not rely on behavioral inference or engagement maximization.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Highlights the need for minors to easily access non-profiling recommender system options via the platform interface.

The DSA states that VLOPS and VLOSEs need to provide alternative options for recommender systems which are not based on profiling (Article 38) and that "such choices should be directly accessible from the online interface where the recommendations are presented" (recital 94).

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Supports exploration of non-profiled content for minors, but argues obligations should be limited to very large platforms to avoid burdening smaller providers.

However, the Guidelines effectively expand the obligation to make available options for recommender systems not based on profiling to providers of all online platforms. This goes beyond the legislative intent of the DSA, and would represent a disproportionate burden for providers of smaller online platforms.

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 (European Commission). Stresses the importance of avoiding ongoing or off-platform behavioral data collection in recommendations for minors and empowering them to choose non-profiling options.

Ensure that recommender systems do not rely on the on-going collection of behavioural data that captures all or most of the minor's activities on the platform, such as watch time and click through rates, and do not rely on the collection of any behavioural data that captures the user's activities off the platform.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Advocates for a rights-based approach, including user control and a range of cumulative safeguards in recommender system design for minors.

La CNCDH promeut depuis plusieurs années la consécration d'un droit au paramétrage des contenus reçus, par une reprise en main de l'utilisateur sur les systèmes de recommandation à l'œuvre sur les plateformes.

Joint Statement on Article 28 Guidelines (5Rights Foundation). Urges that default recommender system settings for minors avoid user profiling while ensuring child-appropriate design.

the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Warns against outright bans on behavioral data in minors' recommender systems due to the risk of diminishing service quality and appropriateness.

However, we are concerned that the draft Guidelines may inadvertently limit service providers' ability to deliver safe and developmentally appropriate experiences for minors by recommending the outright prohibition of behavioural data in recommender systems (Section 6.5):

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Highlights the necessity of prioritizing explicit user signals in recommendation for minors, justified in their best interests.

Prioritise 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Restates the need for non-user profiling as default in recommender systems for children, maintaining child-friendliness.

the non-user profiling recommender system option should be made the default setting while ensuring that it remains child-friendly.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Asserts that recommender systems for minors should default to explicit, user-provided signals for a positive user experience.

Save the Children considers crucial that recommender systems based on 'explicit user- provided signals' should be made the default setting for children, to effectively translate active user signals into a positive user experience.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). Recommends personal feeds for minors be based on accounts they actively follow and that recommender systems be shown only upon conscious choice by the minor.

Im Hinblick auf die in den Leitlinien auch genannten Risiken, die Empfehlungssysteme für Kinder und Jugendliche darstellen können, regen wir an, dass diese Liste der Voreinstellungen im Hinblick auf den persönlichen „Feed“ insofern erweitert wird, dass als Grundeinstellung vornehmlich Inhalte von Konten angezeigt werden, denen der Minderjährige aktiv folgt.

1.8.3 User Control and Transparency

Across these documents, there is broad consensus that recommender systems for minors should be designed to maximize user control and transparency. Key recommendations include ensuring that minors (and sometimes their guardians) have accessible and intuitive options to reset, modify, or opt out of personalized recommendations entirely; these controls should be tailored to be child-friendly and easily found in platform interfaces. Another ongoing concern is the need for meaningful, comprehensible, and age-appropriate explanations of why content is recommended, with calls for explainability that avoids overwhelming minors with information. Additionally, there is advocacy for the impact of reporting and feedback mechanisms to be prompt and measurable, so that the recomender’s outputs reflect user preferences in a tangible way. Some documents extend the discussion toward the structural aspects of recommender design, urging platforms to provide clearer segregation (such as followed vs. non-followed feeds), encourage explicit user input (while recognizing operational limitations), and even allow users to choose between a range of third-party recommender systems aligned to their privacy or content preferences. Transparency is not only about information provision but also about concrete and protective defaults, especially given the vulnerabilities of minors online. Thus, typical insights focus on easy-to-use, effective, and transparent user interfaces for managing recommendations, robust explainability tailored to minors, and mechanisms to ensure user feedback directly influences visible recommendations, all underpinned by a principle of safeguarding and empowering young users.

Provide minors with the opportunity to reset their recommended feeds completely and permanently." (CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe))

Explain why each specific piece of content was recommended to them, including information about the parameters used and the user signals collected for that specific recommendation. Providers should also provide information to minors about prompts that encourage minors to search for new content after a certain period of time interacting with the recommender system. This information should be child-friendly and accessible (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 (European Commission))

Those settings should be easy to find and to use, minor friendly. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

A case study examined by the Panoptykon Foundation demonstrates how Facebook uses algorithms to deliver personalized ads that may exploit users' mental vulnerabilities. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Explain why each specific piece of content was recommended to them, including information about the parameters used and the user signals collected for that specific recommendation. Providers should also provide information to minors about prompts that encourage minors to search for new content after a certain period of time interacting with the recommender system. This information should be child-friendly and accessible (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 (European Commission))

There needs to be a way for users to express negative feedback that is as easy, and effective, as liking something. (European Commission Article 28 Guidelines Feedback (unknown))

EFPA contribution to consultation on the protection of minors guidelines (European Federation of Psychologists' Associations (EFPA)). Recommends treating recommender systems that strongly influence minors as high-risk and calls for genuinely child-friendly explanations of algorithmic decisions that go beyond simple justifications.

Beyond stating that platforms should explain why content was recommended, it could encourage the development of genuinely child-friendly explanations of how algorithmic decisions are made.

Salminen contribution protection of minors (Aalto University). Highlights that algorithmically amplified feeds can undermine minors' ability to make informed choices, recommending a strict separation between followed and non-followed content feeds for children.

Thereby, this research recommends strictly separating the followed and non-followed feeds for child accounts.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Encourages transparency and accountability in recommender system designs, emphasizing their role in reducing online polarization and supporting democratic engagement.

Designing Recommender Systems to Depolarize."

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Shows that users often lack meaningful control over algorithmic curation, with platforms exposing users to unwanted or even disturbing content despite opt-out attempts.

The study found Facebook's algorithms expose users to disturbing, trauma-related content despite their efforts to opt out, revealing that the platform does not give users meaningful control over what they see.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Advocates that minors should have the ability to completely and permanently reset their recommended feeds, viewing this as a universal tool for all platforms.

Provide minors with the opportunity to reset their recommended feeds completely and permanently."

Safe by Default (Panoptykon Foundation). Calls for default promotion of user education on customization and for VLOPs to improve transparency and user control in recommender systems.

By default VLOPs should promote these features and educate their users about ways to customise their experience.

DOT Europe response1 (DOT Europe). Suggests the need for more specific, practical guidance on how to explain recommender systems to minors without causing information overload.

With this in mind, more specific guidelines or examples on what constitutes adequate explanations about recommender system mechanisms and how platforms should practically ensure minors understand this information would be useful.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Favors prioritizing explicit user signals when capturing user preferences for recommendations, while acknowledging the logistical challenges of large-scale user feedback collection.

We highly encourage the use of explicit signals over implicit signals, but want to note the challenges for platforms to implement effective user surveys.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Recommends clear, easy-to-use controls allowing minors to opt out of personalized recommendations or to limit the categories of recommendations they receive.

control personalized recommendation systems, including the ability for a minor to have- (i) a prominently displayed option to opt out of such personalized recommendation systems, while still allowing the display of content based on a chronological format; and (ii) a prominently displayed option to limit types or categories of recommendations from such systems;

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Welcomes reset options for children's recommender systems but underscores that such controls must be truly accessible and age-appropriate.

However, it needs to be ensured that those options are easily available and child-friendly.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Endorses transparent and protective-by-default recommender systems for children, with easy options for minors/guardians to reset or adjust settings without frequent re-prompts.

la Commission demande à juste titre aux plateformes en ligne de « donner aux mineurs la possibilité de réinitialiser complètement et définitivement leurs flux recommandés ». (p. 1

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). States the need for minors to have accessible tools to reset their recommended feeds and revert to prior versions, recognizing this as essential across all platforms.

Provide minors with the opportunity to reset their recommended feeds completely and permanently."

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 (European Commission). Mandates child-friendly explanations for recommendations and ensures that feedback and reporting from minors rapidly and durably changes recommendation outputs.

Explain why each specific piece of content was recommended to them, including information about the parameters used and the user signals collected for that specific recommendation. Providers should also provide information to minors about prompts that encourage minors to search for new content after a certain period of time interacting with the recommender system. This information should be child-friendly and accessible

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Supports user empowerment in recommender systems and advocates for platforms to give users (including minors) the option of choosing among different recommendation algorithms.

The DSA allows users to easily choose between different recommendation systems when multiple options are available.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Recommends that all settings for controlling recommender systems should be minor-friendly and easy to locate, with specific options for minors to adjust their content preferences.

Those settings should be easy to find and to use, minor friendly.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Supports full and permanent reset options for minors and suggests platforms could implement periodic, automatic resets to help prevent harmful content loops.

We also support that platforms should "provide minors with the opportunity to reset their recommended feeds completely and permanently" (line 579), as this is a crucial step to prevent users from falling into harmful content loops or "rabbit holes."

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Affirms the importance of complete and permanent reset capabilities for minors' recommended feeds to protect them from algorithmically driven rabbit holes.

We support that platforms should provide minors with the opportunity to reset their recommended feeds completely and permanently (line 579), as this is a crucial step to prevent users from falling into harmful content loops or rabbit holes.

European Commission Article 28 Guidelines Feedback (unknown). Calls for feedback mechanisms to be as straightforward as liking content and for their effects to be immediate, observable, and confirmed through follow-up with minors.

It should be one click easy for a teen to say a piece of content is not for them, and then to be offered the option of similar content not being recommended to them, and the effect of the feedback being immediate, and measured by asking the minor later if that tool is effective, and if their preferences are being respected.

1.8.4 Platform and Context Specificity

The category "Platform and Context Specificity" within recommender systems and personalization highlights the need for tailored, context-aware approaches when designing and regulating recommendation technologies, particularly for the protection of minors. A key insight across documents is the significant diversity in both the types and purposes of recommender systems (e.g., content vs. product recommendations), their associated risks, and the platforms on which they operate. As such, several stakeholders caution against one-size-fits-all regulatory guidelines under frameworks like the Digital Services Act (DSA), urging instead for proportionate, risk-based measures that reflect both platform-specific and recommender-specific factors. Contributions also stress that effective policy must account for contextual nuances, such as the popularity of certain platforms among minors, the locality of content (using locality-aware algorithms to foster community engagement), and the potential for positive and protective uses of recommender systems. There is also a call for greater clarity regarding definitions (e.g., what constitutes "profiling") and the interplay of recommendation and moderation mechanisms under legal frameworks to avoid unnecessary burdens or unintended consequences. Overall, the consensus is that sound governance of recommender systems must recognize the range of system designs, operational contexts, and user needs (including minors' accessibility and safety), employing targeted mitigations and promoting platform accountability, rather than imposing blanket or ill-defined requirements.

The guidelines should clarify that mitigation measures do not apply in equal measures across all online platforms. (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))

Instead, Online Platforms should assess the specific risks of their recommender system and implement proportionate and targeted risk mitigation strategies. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

Rather than imposing blanket requirements, the Commission should establish principles that allow each online platform to tailor measures to the specifics of their recommender systems, in a way that is flexible enough to appropriately mitigate the risks. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

Acknowledging the constructive potential of system settings and design features, as well as mitigation measures, supports a more balanced and nuanced approach as mitigation mechanisms and enables platforms to use all available tools to protect minors online. (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))

Recommender systems can then be tailored, for example, to prioritise and promote content, in the case of children, that can be age-appropriate, educational, and enriching content. (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))

The recommendations should particularly target social media platforms that are popular among younger audiences, such as Discord, Habbo, Hotel Hideaway, and Steam as well as social media platforms the qualify as very large under the DSA. (Salminen contribution protection of minors (Aalto University))

Stellungnahmen zum Leitlinienentwurf zum Minderjährigenschutz im Digital Services Act (Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)). Advocates for distinguishing between content and product recommendation systems, arguing that applying the same risk mitigation to both fails to reflect their different functions and risks.

Die Kommission sollte deshalb der unterschiedlichen Natur von Inhalts- und Produktempfehlungen hinreichend Rechnung tragen und Onlineplattformen erlauben, die spezifischen Risiken ihrer Empfehlungssysteme im Einklang mit den Leitlinien zu bewerten und verhältnismäßige und gezielte Strategien zur Risikominderung umzusetzen.

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Urges the adoption of nuanced, risk-based controls in platform regulation, highlighting the diversity of recommender systems and the importance of balancing risks with potential benefits, especially for minors.

Recommender systems vary widely in nature and application, and consequently so does their risk level.

Salminen contribution protection of minors (Aalto University). Emphasizes that regulatory attention should focus particularly on platforms with significant minor user bases, especially large, popular social platforms, for effective protection.

The recommendations should particularly target social media platforms that are popular among younger audiences, such as Discord, Habbo, Hotel Hideaway, and Steam as well as social media platforms the qualify as very large under the DSA.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Proposes locality-aware algorithms to ensure users receive content relevant to their geographic context, supporting local engagement and civic participation.

Locality-aware algorithms prioritize content contextually relevant to a user's geographic location.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Calls for mitigation measures to be proportionate and targeted to recommender-specific risks rather than being universally applied to all platforms.

Instead, Online Platforms should assess the specific risks of their recommender system and implement proportionate and targeted risk mitigation strategies.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Argues for platform flexibility to tailor recommender system measures based on specific platform risks, opposing blanket requirements that may impact user experience.

Rather than imposing blanket requirements, the Commission should establish principles that allow each online platform to tailor measures to the specifics of their recommender systems, in a way that is flexible enough to appropriately mitigate the risks.

Feedback DSA (unknown). Seeks clarification on policy regarding whether minors should be shown adult-created content or content from trusted sources in recommendation feeds.

Clarify whether adult-created content should be shown to minors or if the system should default to content produced by verified peers or trusted sources.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Highlights the need to clarify how content restriction measures in recommender systems interact with existing DSA requirements to avoid disproportionate administrative burdens.

This seems disproportionately burdensome, and the interaction with DSA Articles 16 and 17 should at the very least be clarified here.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Recommends explicitly listing the types of recommender systems covered by guidelines and considering the accessibility and diverse needs of minors in design objectives.

e suggest the guidelines including the line: "Relevant recommender systems include, but are not limited to, those used for content feeds, search results, ads display, notifications, comment feeds, and others."

1.8.5 Content Diversity and Quality

This category focuses on enhancing the diversity and quality of content surfaced by recommender systems, especially for minors. Key themes include the importance of exposing users—particularly children and adolescents—to a wide array of age-appropriate, educational, and developmentally beneficial content, rather than narrowly optimizing for engagement or allowing algorithms to reinforce echo chambers and filter bubbles. Several insights call for explicit interventions, such as content diversification protocols, exposure diversity algorithms, and prompts that encourage users to seek new content after prolonged interaction, aiming to disrupt repetitive or high-stimulation content cycles. There is a strong emphasis on ensuring that recommender systems not only respect but actively promote user wellbeing and personal development. Recommendations include balancing minors' self-directed choices with expert-curated content, prioritizing trusted and prosocial sources, and providing transparency and user control over recommendation logic. Concerns are also raised about commercial and polarizing biases in algorithmic systems, as well as the risk of narrowing minors' exposure to new interests and potentially stifling personal growth. Diverse viewpoints, civil discourse, and factual accuracy are highlighted as crucial aspects of quality content, while guidance is proposed for platforms to steer users toward authoritative sources on sensitive or public interest topics.

Recommender systems should be designed so that no more than a specified number of consecutive pieces of similar high-engagement content are shown before introducing educational, calming, or offline-encouraging content designed to promote digital wellness or learning. (Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz))

To further ensure that online platforms act in the best interests of children, we suggest strengthening this section, particularly the prompt in lines 581-582, to encourage platforms to actively provide minors with new and diverse content. (UNICEF Sweden's comments on the protection of minors guidelines under the Digital Services Act (UNICEF Sweden))

Exposure Diversity Algorithms aim to reduce echo chambers and promote cognitive empathy by diversifying what users see. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

highlight content that receives positive responses across the political spectrum and present users with more content that resonates with a wide range of audiences from different groups; (Safe by Default (Panoptykon Foundation))

Exposure Diversity Algorithms aim to reduce echo chambers and promote cognitive empathy by diversifying what users see. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

If recommender systems were solely dictated by a minor's immediate and explicit preferences, they might not consistently receive the most high-quality, enriching, or developmentally beneficial content. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Avaaz advocates for implementing content diversification protocols in recommender systems for minors, ensuring that content recommendations alternate between entertaining and educational or calming materials to support digital wellness.

Recommender systems should be designed so that no more than a specified number of consecutive pieces of similar high-engagement content are shown before introducing educational, calming, or offline-encouraging content designed to promote digital wellness or learning.

UNICEF Sweden's comments on the protection of minors guidelines under the Digital Services Act (UNICEF Sweden). UNICEF Sweden encourages platforms to actively provide minors with diverse, high-quality, and authentic content and highlights children's desire to escape poorly calibrated and commercialized recommender feeds.

To further ensure that online platforms act in the best interests of children, we suggest strengthening this section, particularly the prompt in lines 581-582, to encourage platforms to actively provide minors with new and diverse content.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild underscores the importance of ensuring that recommender systems promote access to a diversity of relevant, age-appropriate information that advances children's rights and development.

Ensure that recommender systems promote minors' access to a diversity of age-appropriate information that is relevant and adequate for them, with due consideration to their age group.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). The Blueprint on Prosocial Tech Design argues for prosocial algorithms that boost the diversity of viewpoints, improve discourse quality, and use exposure diversity strategies to reduce echo chambers and support societal cohesion.

Exposure Diversity Algorithms aim to reduce echo chambers and promote cognitive empathy by diversifying what users see.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). This extended blueprint details how recommendation algorithms can be reoriented to incentivize trusted sources, fairness, and agreement between groups, and implement civility- and credibility-focused ranking to improve content quality.

Prosocial algorithms and recommender systems could reorient social media to enhance the social fabric by helping people experience a wider diversity of viewpoints and discover more context.

Safe by Default (Panoptykon Foundation). The Panoptykon Foundation proposes measurable diversity as a metric of success for recommender systems, advocating for balanced information exposure and prominent guidance to authoritative sources on sensitive or public interest topics.

Introducing diversity as a metric of success for a recommender system and making sure that the stream of personalised recommendations includes a range of topics, instead of exploiting the one that is most engaging for the user in a given moment.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Google highlights the need to balance minors' explicit preferences with content expert guidance, to ensure minors are exposed to high-quality, developmentally beneficial content instead of just entertaining material.

Minors, by nature of their age and cognitive development, may primarily gravitate towards content that is immediately entertaining, trending, or superficially engaging.

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 (European Commission). The European Commission suggests promptings for minors to seek new content after extended engagement with recommender systems, aiming to diversify their digital experience.

Provide prompts for the minor to search for new content after a certain amount of interaction with the recommender system.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Electronic Frontier Foundation calls for platforms to foster content plurality, transparency, and user control in recommendation systems, while cautioning against the unilateral definition of what is 'relevant and adequate' for minors.

Instead, the guidelines should encourage platforms to prioritize content plurality.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). CNCDH stresses promoting age-appropriate and respectful sexual and affective education content, warning that current algorithmic models often sideline such material in favor of polarizing content.

le modèle économique des plateformes, qui valorise des contenus polarisants, contribue également à la sous-représentation de contenus ou de créateurs de contenus susceptibles de donner aux enfants les moyens de développer des relations affectives et sexuelles respectueuses.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). TikTok supports measures to prompt minors to search for new content after certain intervals, aiming to ensure privacy, safety, and content diversity.

measures to ensure a high level of privacy, safety and security of minors: . Provide prompts for the minor to search for new content after a certain amount of interaction with the recommender system.

On the concept of personal integrity in the german protection of minors (unknown). The German analysis addresses the risk that algorithms can restrict children's development by limiting exposure to diverse content and suppressing the discovery of new interests.

As a result, there is a risk that potential new interests and talents may remain undiscovered or be hindered.

1.8.6 Safety and Risk Mitigation

This collection of insights underscores a comprehensive approach to recommender system safety and risk mitigation for minors. A strong consensus emerges around the need for both proactive and reactive safeguards: measures to prevent exposure to illegal and harmful content, avoidance of addictive designs, and stricter handling of suspicious or criminal accounts. Many recommend periodic and participatory impact assessments involving children and independent experts, with systems adapted based on such findings. A crucial thread is the importance of balancing strict safety measures with the positive potential of recommender systems, advocating for risk-proportionate, targeted interventions rather than blanket restrictions. Approaches include introducing 'positive friction,' prompts for mindful disengagement, and ensuring algorithmic transparency and accountability. Notably, several contributions emphasize the value of fostering digital well-being, reducing risk of addiction, excessive influence, and social comparison, and encouraging platforms to actively support minors' rights and healthy online development. Finally, there is debate on operational specifics—such as when to prohibit recommendations, how to factor in behavioral data, and the extent to which platforms should prioritize content from minors' networks. Together, these documents reveal a nuanced landscape prioritizing safety, agency, inclusivity, and well-being in recommender system design for children.

Implement measures to prevent a minor's repeated exposure to content that could pose a risk to minors' safety and security, particularly when encountered repeatedly, such as content promoting unrealistic beauty standards or dieting, content that glorifies or trivialises mental health issues, such as anxiety or depression, discriminatory content, illegal content and distressing content depicting violence or encouraging minors to engage in dangerous activities. (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 (European Commission))

Include prompts encouraging new content searches after extended use (Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz))

In the opinion of our organisations, any account under investigation for impersonation needs to be categorically excluded from recommendation algorithms. (Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE))

Implement inverse engagement prioritization for harmful content, ensuring that high-risk content receives lower algorithmic priority even when it generates high user engagement, thereby breaking the cycle where dangerous content becomes more addictive and widely distributed. (Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz))

Recommender systems should by default not connect minors with adults (Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn))

Implement measures to ensure that recommender systems do not enable or facilitate the dissemination of illegal content or the commitment of criminal offences against minors. (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 (European Commission))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Stresses the need to extend harmful content restrictions and prevention of addictive use for minors in recommender systems, and advocates non-profiling options and user prompts to help manage engagement.

Include prompts encouraging new content searches after extended use

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Introduces digital well-being strategies, such as 'Digital Nutrition Scoring Algorithms,' to foster psychological health and mindful screen usage via content recommendations.

Digital Nutrition Scoring Algorithms optimize for user health and mindfulness by recommending content that improves psychological health, empathy, and civic knowledge-like a "healthy diet for the mind."

Safe by Default (Panoptykon Foundation). Recommends the use of 'positive friction' to slow down user engagement and mitigate addictive behaviors by inserting breaks and 'think before you share' messages.

Platforms should introduce positive friction aimed at slowing down posting and user interactions, giving users a chance to think before sharing.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Emphasizes platform responsibility to deter children’s involvement in criminal activities via recommender systems and calls for explicit integration of this consideration in guidelines.

Bris would like to emphasize that platforms also have a responsibility to prevent children from becoming involved in criminal activities.

DOT Europe response1 (DOT Europe). Argues that risk mitigation measures should be proportional to the specific risk profiles of different recommender systems, not universally applied.

The proposed mitigations suggested in Section 6.5 are tailored to the specific risks posed by content recommender systems specifically.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Urges extension of safeguards to cover both harmful and illegal content or contacts and highlights prevalence of harmful recommendations on popular children's platforms.

We suggest adding an explicit reference not only to "illegal" but also to "harmful" content or contacts.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Advocates for risk-based, targeted mitigation for recommender systems, recognizing their varied nature and associated risks.

Recommender systems vary widely in nature and risk level, such as content and product recommendation systems.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Suggests categorically excluding accounts under impersonation investigation from minors' recommendation algorithms to bolster safety.

In the opinion of our organisations, any account under investigation for impersonation needs to be categorically excluded from recommendation algorithms.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Recommends an explicit prohibition on recommending suspicious accounts to minors as a proportionate safety safeguard.

Lastly, the text should explicitly prohibit algorithmic recommendation of suspicious accounts to minors.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Calls for regular assessment and adaptive modification of recommender systems' impacts on children, including in consultation with minors and stakeholders.

Recommender systems should be regularly assessed as to their impact and adapted accordingly.

Feedback DSA (unknown). Advises disabling recommendation systems and pop-ups that could steer minors toward risky or unrelated content, instead prioritizing content from minors' own networks.

Turn off content recommendation systems and pop-ups that direct minors to unrelated or risky content.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Advocates that by default recommender systems should not connect minors with adults, aiming to reduce unwanted exposure and contacts.

Recommender systems should by default not connect minors with adults

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Recommends regular impact assessments of recommender systems on children's rights, with independent expert and child involvement.

we recommend that the guidelines go further in requiring providers of online platforms to regularly assess and document the real-world impact of their recommender systems on children's rights – including the right to information, participation and protection.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Suggests implementation of behavioral analysis to detect potentially addictive usage and promote diversity and reflection in content for minors.

Empfehlungsalgorithmen gelten als Schlüsselmechanismus für exzessive Nutzung, da sie Inhalte kontinuierlich nachliefern, die maximale Aufmerksamkeit binden.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Promotes use of prompts to encourage minors to seek new content after repeated interactions to prevent rabbit-hole effects and addictive engagement.

Provide prompts for the minor to search for new content after a certain amount of interaction with the recommender system".

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 (European Commission). Stresses implementation of measures to prevent repeated exposure to harmful or flagged content and prevent distribution of illegal content through recommender systems.

Implement measures to prevent a minor's repeated exposure to content that could pose a risk to minors' safety and security, particularly when encountered repeatedly, such as content promoting unrealistic beauty standards or dieting, content that glorifies or trivialises mental health issues, such as anxiety or depression, discriminatory content, illegal content and distressing content depicting violence or encouraging minors to engage in dangerous activities.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Proposes reduction of social comparison and trend amplification by recommender systems, coupled with regular and participatory system impact evaluations.

Recommender systems must reduce social comparison and trend amplification.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Highlights the benefits of recommender systems in providing age-appropriate content and calls for a balanced, risk-based approach rather than an exclusive focus on risks.

Recommender systems help users navigate vast amounts of information and can promote access to high- quality, trustworthy, and age-appropriate content.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Asserts that guidelines should allow use of behavioral data to enhance safety for minors and encourages risk assessment-based application of safeguards.

We are concerned, therefore, that the proposed guidelines on recommender systems and search features are overly prescriptive and deviate from the risk-based approach enshrined in Articles 34 and 35 of the DSA.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Advocates for a ban on algorithms that forcibly push uncontrollable digital content, specifically to protect children and young people from risk exposure.

Jveren voor: (1) het verbieden van algoritmes en mechanismen die de gebruiker oncontroleerbare digitale content opdringt; die kinderen en jongeren blootstelt aan risico's zoals verslaving, ongepaste inhoud of afstompende filmpjes;

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Argues for recognition of recommender system benefits for minors and that mitigation efforts should only target identified risks, not personalization as a whole.

The "Guidelines" should acknowledge this positive impact beyond just focusing on risks.

1.8.7 Child and Age-Appropriate Personalization

Across the reviewed documents, there is widespread recognition of the need for child- and age-appropriate personalization in recommender systems. Key insights include the importance of prioritizing minors' safety and developmental needs above pure algorithmic relevance or engagement, recommending that systems promote access to content that is both adequate and age-appropriate. Many stakeholders argue for personalization models that either default to or heavily emphasize explicit user-provided signals and settings—allowing minors to actively shape their feeds and experiences, for example, by making it easy to reset recommendations or provide direct feedback on content suitability. A strong theme is the call for robust privacy protections and data minimization in personalization for minors, often limiting or strictly regulating behavioral tracking. Some documents also highlight that personalization, when handled responsibly, can improve minors' safety and wellbeing by surfacing valuable and positive content and reducing exposure to risks, provided privacy and purpose limitation safeguards are in place. Ongoing evaluation, transparency, and collaboration (including with children) are recommended to assess the actual impact of recommender systems on minors. Finally, several contributions underscore that both recommender system design and controls should reflect the evolving capacities of children and include age-differentiated strategies.

Provide minors with the opportunity to reset their recommended feeds completely and permanently, in an accessible and age-appropriate manner. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

The NMA suggests deleting "relevant" to put more weight on "adequate": "Ensure that recommender systems promote minors' access to information that is relevant and adequate for them, with due consideration to their age group. (The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority))

Recommender systems offer significant value in helping minors discover enriching and age-appropriate content. (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))

Meaningful engagement can support a minor's development. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

The value of personalisation in enhancing minor safety is recognised. However, potentially restricting the collection of certain data useful for tailoring content could harm safety. (DOT Europe response1 (DOT Europe))

In particular, the recommendations in the Guidelines that providers should minimise the collection of behavioural data (L 535 - 538), or prioritise certain signals over others (e.g. L 539 - 550, L 565 - 567), risk undermining these benefits. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates for giving minors an accessible, age-appropriate way to reset their personalized recommendation feeds, empowering them to manage their online experiences autonomously.

Provide minors with the opportunity to reset their recommended feeds completely and permanently, in an accessible and age-appropriate manner.

The Norwegian Media Authorities' Feedback to the Draft Guidelines to DSA's article 28 (Norwegian Media Authority). Emphasizes that recommender systems for minors should prioritize not just relevance but adequacy, ensuring content is appropriate for different age groups.

The NMA suggests deleting "relevant" to put more weight on "adequate": "Ensure that recommender systems promote minors' access to information that is relevant and adequate for them, with due consideration to their age group.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Highlights the positive impact of recommender systems in helping minors discover enriching, trustworthy, and age-appropriate content, while stressing the need for privacy safeguards in behavioral data use.

Recommender systems offer significant value for minors discovering high-quality content; personalization highlighting high-quality and trustworthy content is crucial for that and should be recognised in the guidelines.

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Recognizes the dual role of behavioral data: it enables appropriate recommendations for minors while necessitating strong protection of minors' personal data and tailored risk mitigation.

Personalised recommendations can also help reduce repeated exposure to certain content that, while harmless when viewed once, may become problematic with excessive viewing.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Calls for platforms to regularly evaluate and document the effects of recommender systems on children's wellbeing, involving experts and children themselves in these assessments, and for regular, clear reminders about feed-resetting options.

we believe the guidelines could go further by requiring platforms to regularly evaluate and document the impact these systems actually have on children's wellbeing and children's rights.

DOT Europe response1 (DOT Europe). Warns that restricting data collection for personalization could inadvertently harm minors' safety, as effective personalization can be protective when carefully managed.

The value of personalisation in enhancing minor safety is recognised. However, potentially restricting the collection of certain data useful for tailoring content could harm safety.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Recommends that recommender systems for minors should avoid behavioral profiling and engagement-maximizing algorithms, relying instead only on explicit preferences from the minor.

Recommendation algorithms often prioritise content that maximizes engagement. This model can expose children to disturbing, addictive, or extreme content.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Suggests that behavioral data can be used for minors' personalization, but only under strict safeguards with clear purposes, and urges against blanket prohibitions that discard valuable risk-mitigation tools.

Rather than a categorical prohibition, providers should be permitted to use behavioural data for the specific purpose of enhancing child safety and delivering age-appropriate experiences, provided such use is clearly defined and subject to appropriate safeguards.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Argues that safe defaults and limited, safety-focused choices are necessary, as minors cannot be relied upon to configure privacy and personalization settings themselves.

Minor users should be presented with a limited set of choices, all of which prioritize safety.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Supports the idea that recommender systems help minors discover age-appropriate content and recommends guidelines reflect this benefit, balancing personalization with privacy protections.

Recommender systems offer significant value in helping minors discover enriching and age-appropriate content.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Supports prioritizing explicit user input over implicit signals for minors' recommendations, ensuring that recommendations align with minors' best interests and foster a healthier online experience.

By prioritising 'explicit user-provided signals' over 'implicit engagement-based signals' to determine the content displayed and recommended to minors, the Commission has required that such signals should be justified in the best interest of the minor, which will help to ensure that the signals contribute to a high level of safety and security for minors.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Advocates defaulting children's recommender systems to rely on explicit user signals, ensuring interfaces are user-friendly and encourage positive engagement.

Recommender systems based on 'explicit user-provided signals' should be defaulted for children, ensure that this feed is child user-friendly and effectively translates active user signals into a positive user experience.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Recommends tailoring

design and evaluation of recommender systems to children's various developmental stages, adapting strategies by age group.

Furthermore, design and evaluation strategies should be differentiated by age group and reflect the evolving capacities of children.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Welcomes the guidelines' recognition of recommender systems' significant value for minors, noting that responsive personalization can foster positive online engagement.

We welcome that the Guidelines acknowledge the significant value of recommender systems, not only for adult users, but also for minors.

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 (European Commission). Stresses that minors' feedback should actively shape content ranking in recommender systems, and demands that all system interfaces for minors be accessible and child-friendly.

For example, minors' feedback about content, activities, individuals, accounts or groups that make them feel uncomfortable or that they want to see more or less of should be taken into account in the ranking of the recommender systems.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Proposes a ban on algorithmic recommenders for under-18s in favor of neutral or chronological content feeds, requiring content discovery to be user-initiated.

Vodafone strongly recommends that the guidelines mandate that algorithmic recommender systems in platforms are not activated for under 18s and these users instead experience a neutral/chronological home page, where content discovery is initiated by user search terms and commands.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Supports age-appropriate recommender systems but seeks clarification on how and how often platforms must fulfill these requirements.

Safer Internet Centre Denmark supports age-appropriate recommender systems, call on the Commission to clarify how often and in what ways platforms should comply with these requirements to make them effective.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Calls for recommender and search system design, privacy, and explainability measures that reflect developmental appropriateness and prioritize minors' best interests.

the systems and online search features must be aligned with the requirements in age- appropriate guidelines, such as documenting developmental appropriateness in interfaces and content design, by default supporting privacy by design and default for minors, maintaining data minimization with limitations on profiling of minors, providing transparency and explainability tailored to minor's cognitive capacity and use as a guiding principle - what's in the best interest of the child.

1.8.8 Miscellaneous

The 'Miscellaneous' category in Recommender Systems and Personalization encompasses nuanced considerations regarding regulatory expectations and practical measures for handling minors' data and personalization online. It highlights ongoing ambiguities in interpreting guidelines for recommender systems—especially concerning the use, scope, and prioritization of behavioral data, both explicit and implicit, in recommendations for minors. There is a call for clearer definitions and proportionality in implementing such measures, ensuring that legal requirements do not unnecessarily over-restrict beneficial personalization. Additionally, stakeholders express concerns over certain suggested practices—like offering minors the permanent ability to reset recommendation feeds or frequent prompts to reset or search—as possibly exceeding actual regulatory obligations under the DSA. They suggest such options could remain as best practices rather than mandatory compliance checks, emphasizing the need for flexibility in interpreting the guidelines to match legislative intent.

For the proposal in line 535-538 "Ensure that recommender systems do not rely on the on-going collection of behavioural data that captures all or most of the minor's activity on the platform, such as watch time and click through rates, and do not rely on the collection of any behavioural data that captures the user's activities off the platform" it is unclear how to understand that measure, e.g. it is ambiguous what is covered by "rely", "ongoing" and " all or most". (Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.))

Likewise for the proposal in line 539-540 to "prioritise explicit user provided signals over implicit engagement-based signals" it is rather unclear what this entails. We understand it means that implicit signals could still be used. (Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.))

some measures listed in the guidelines - such as providing minors with the opportunity to reset their recommended feeds completely and permanently, or providing prompts for the minor to search for new content after a certain amount of interaction with the recommender system - clearly go beyond the scope of the DSA, even its obligations for VLOPs. (Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe))

For the proposal in line 535-538 "Ensure that recommender systems do not rely on the on-going collection of behavioural data that captures all or most of the minor's activity on the platform, such as watch time and click through rates, and do not rely on the collection of any behavioural data that captures the user's activities off the platform" it is unclear how to understand that measure, e.g. it is ambiguous what is covered by "rely", "ongoing" and " all or most". (Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.))

some measures listed in the guidelines - such as providing minors with the opportunity to reset their recommended feeds completely and permanently, or providing prompts for the minor to search for new content after a certain amount of interaction with the recommender system - clearly go beyond the scope of the DSA, even its obligations for VLOPs. (Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe))

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Meta Platforms points out the ambiguity in draft regulatory language regarding recommender system data practices for minors, arguing for clearer distinctions between requirements and for proportionality so user-relevant personalization is not unduly restricted.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Middle Tech Europe argues that some guideline recommendations, such as letting minors permanently reset their recommendation feeds, exceed what is required under the DSA and ought to be considered optional best practices rather than compliance standards.

some measures listed in the guidelines - such as providing minors with the opportunity to reset their recommended feeds completely and permanently, or providing prompts for the minor to search for new content after a certain amount of interaction with the recommender system - clearly go beyond the scope of the DSA, even its obligations for VLOPs.

1.9 AI and Automated System Governance

The most compelling insight across the sub-categories is the broad consensus on the urgent need for enforceable, child-specific protections in AI governance—particularly through mandatory standards, strict oversight, and transparency. Key measures include pre-launch testing, clear disclosures ("age-appropriate notifications"), risk classification systems, and robust labeling requirements for AI-generated content. There is an especially strong call for independent oversight and for aligning regulatory frameworks such as the Digital Services Act, GDPR, and EU AI Act to close jurisdictional loopholes and address the unique risks posed to minors. Transparency and accountability recur as essential pillars: all stakeholders underscore the importance of real-time notifications and opt-out mechanisms, not just for awareness but for actionable control over AI interactions. Explicit attention is given to prohibiting manipulative or emotionally exploitative features, limiting unsolicited recommendations, and implementing protections directly addressing children's rights and

developmental needs. Fairness and bias mitigation are also prioritized, with requirements for regular audits and the use of dedicated toolkits to detect, document, and reduce discriminatory outcomes—especially in high-stakes areas impacting youth. Across sub-categories, dominant trends include a proactive, precautionary orientation and the demand for harmonized, comprehensive governance measures. These are united by a commitment to safeguarding the rights, safety, and well-being of minors, ensuring that risk management, transparency, and ethical design are intrinsic to all stages of AI system development and deployment.

1.9.1 AI Regulation and Legal Compliance

The category "AI Regulation and Legal Compliance" focuses on the development, deployment, and oversight of AI systems, especially as they relate to vulnerable groups such as minors. The insights stress the need for mandatory standards, independent oversight, and a harmonized regulatory approach—aligning frameworks like the Digital Services Act (DSA), General Data Protection Regulation (GDPR), and the EU AI Act—to address the unique risks AI tools pose to children. Many contributions advocate for pre-launch testing, transparency, explainability, and human oversight of AI systems, especially on platforms accessible to minors. Special attention is given to issues like the use of AI chatbots and recommendation systems interacting with children, with some documents calling for outright moratoriums on certain AI applications for under-16s, and others highlighting the need for public disclosure of training data and robust warning systems. There are also calls for a classification of AI risk levels and the application of stricter measures for high-risk or manipulative AI systems. Notably, there are discussions about balancing these safeguards with proportionality and practicalities, such as ensuring warnings are contextually appropriate and not overly burdensome. Overall, the documentation reveals a strong emphasis on enforceable, child-specific protections in AI regulation, with a minority viewpoint from industry players suggesting risk-based, rather than absolute, requirements. There's also advocacy for broad EU-wide standards to prevent jurisdictional loopholes, as well as nuanced debates about the ethical limits of AI (e.g., simulated empathy) and the value of transparency and accountability throughout the AI lifecycle.

> *The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.* (CONCLUSION & POLICY DEMANDS (unknown))
>
> *Only mandatory standards with real consequences will protect minors online.* (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))
>
> *In this context, it is essential that the Art. 28 DSA Guidelines are aligned with other relevant legislation such as the GDPR and the EU AI Act.* (Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University))
>
> *Only mandatory standards with real consequences will protect minors online.* (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))
>
> *The Guidelines state that AI features and systems integrated into an online platform should come with a warning to minors that they are interacting with an AI system. This would prevent providers from assessing whether the risk posed by the particular AI system warrants such a warning, and as such, whether such a warning would be an "appropriate and proportionate measure" for the purposes of Article 28(1) DSA.* (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))
>
> *hile AI empathy is fundamentally flawed, its restricted use in specific, low- stakes contexts (e.g., mental health triage, where a chatbot directs users to human therapists) might still serve a purpose without pretending to replace human connection.* (The Case Against AI Simulated Empathy (unknown))

CONCLUSION & POLICY DEMANDS (unknown). This document calls for mandated independent oversight and specific safety requirements in the development, testing, and deployment of AI tools on platforms accessible to minors under the Digital Services Act.

Safe by Default (Panoptykon Foundation). Pushes for EU-wide adoption of rules against toxic algorithms, particularly those embedded in Big Tech platforms, to protect users, including children.

MEPs write to European Commission @ ThierryBreton & @Vestager asking for Irish @CNaM_ie rules against Big Tech's toxic algorithms to be applied across the EU.",

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU)

2022/2065 (Bris). Bris urges clarification that all AI functions integrated into platforms used by children should be governed by the DSA and its safety guidelines.

As indicated in lines 816-818, Al functions that appear to children as an integrated part of a platform must fall under the DSA-and therefore these guidelines.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Contributes calls for stricter regulation of AI interactions with minors, suggesting immediate bans on AI companions for those under 16 and greater transparency regarding AI training data.

Immediate moratorium: No AI chatbots/companions for under-16s

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Reinforces the need for tangible, mandatory standards to safeguard minors online, including a moratorium on AI chatbots for those under 16 and required transparency.

Only mandatory standards with real consequences will protect minors online.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). This document emphasizes the necessity of aligning DSA guidelines with the EU AI Act, especially regarding high-risk systems, to ensure regulatory coherence and comprehensive safeguards.

Include guidance on the intersection of DSA obligations with AI Act requirements for High-Risk AI systems.

Statement - DSA Guidelines (Protect Children). Highlights the mandate for platforms to warn minors when interacting with AI systems, stressing that such measures should cover both deployment and design/creation of these tools.

Section 7.2 covers user support measures and touches on Al features and systems, mandating platforms to "ensure that [...] technical measures are implemented to warn minors that they are interacting with an Al system [...]".

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). COFACE supports references to AI in the DSA guidelines and advocates for increased focus on AI in all aspects of child protection.

However, we believe an additional focus on AI is needed in the guidelines.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Google recommends that requirements to warn minors about AI interactions should be context-dependent and proportionate, rather than always mandatory, to avoid conflicts with existing legal provisions.

This also conflicts Article 50(1) AI Act, which dispenses with the requirement for users to be informed that they are interacting with an AI system in circumstances where this is obvious from the point of view of a reasonably well-informed, observant and circumspect user, taking into account the circumstances and the context of use.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Leiden Law School stresses the importance of aligning DSA guidelines with GDPR and the EU AI Act, with special reference to prohibitions and high-risk AI practices impacting children.

In this context, it is essential that the Art. 28 DSA Guidelines are aligned with other relevant legislation such as the GDPR and the EU AI Act.

The Case Against AI Simulated Empathy (unknown). This piece argues for clear disclaimers and time limits for AI systems simulating empathy, recognizing their limitations, and advocates for strictly regulated, narrowly defined uses.

Even here, the lack of accountability demands strict guardrails-clear disclaimers, time limits, and prompts to seek human support-to avoid fostering dependency.

1.9.2 Ethical Oversight and Risk Management

The key insights from this category emphasize the necessity for robust ethical oversight and risk management in the governance of AI and automated systems, particularly regarding their impact on minors. There is a strong consensus that platforms accessible to children must adopt specific requirements for the safe development, testing, and deployment of AI tools, including chatbots and recommendation systems. Comprehensive independent oversight is repeatedly called for to verify compliance and ensure transparency. Several documents also advocate pre-launch testing, explainability, clear content boundaries, and strict human oversight, with some calling for a moratorium or immediate ban of AI features for minors until adequate testing is confirmed. Additional points raised include the need for risk classification systems to tailor levels of regulation according to potential AI impact, consulting child rights experts, and labelling AI-generated content. The governance framework must also respond to new design-level risks, such as manipulative user experience patterns and potential for harmful content, with mechanisms like expanding bug bounty programs to address these. Collectively, these measures are seen as essential to proactively mitigate the unique risks posed to children by AI systems, protecting their rights, health, and well-being online.

> *The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.* (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))
>
> *The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.* (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))
>
> *The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.* (Ten recommendations to the European Commission to really protect children online (unknown))
>
> *Antisocial design issues like manipulative UX patterns and harmful content amplification are design-level rather than code-level problems.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))
>
> *The deployment of AI tools that interact with minors should be subject to pre-launch testing, explainability requirements, and human oversight procedures.* (Ten recommendations to the European Commission to really protect children online (unknown))
>
> *AI systems can inadvertently offer misleading or developmentally inappropriate suggestions, particularly in response to children's queries related to mental health, relationships, or body image and should therefore be subject to strict content boundaries and human oversight.* (Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår))

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Stresses the need for specific safety requirements and independent oversight for AI tools accessible to minors, highlighting risks such as behavioural influence and advocating for human oversight and tailored regulation.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Reiterates the call for detailed safe development, testing, and independent compliance checks for AI systems accessible to children, emphasizing pre-launch protocols and risk classification.

> *The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.*

Ten recommendations to the European Commission to really protect children online (unknown). Focuses on the inclusion of independent oversight and specific procedures to ensure the safety of minors in the deployment of AI tools on youth-accessible platforms.

The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Advocates expanding traditional cybersecurity bug bounty programs to incentivize identification of ethical design flaws and harms, including those specific to AI and manipulative interface patterns.

Expanding bug bounty programs to include design harms could reward researchers for flagging deceptive patterns and discriminatory systems.

Ten recommendations to the European Commission to really protect children online (unknown). Calls for rigorous requirements and oversight for AI tools used by minors, including bans on untested AI, development of risk classifications, and comprehensive human oversight.

The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.

Policy_demands (unknown). Suggests guidelines should mandate robust safety protocols and third-party oversight for AI systems on child-accessible platforms, noting the unique risks they pose to young users.

The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Argues for a moratorium on AI for minors, citing the prioritization of engagement over safety and the failure of industry self-regulation.

Platforms prioritize engagement over safety.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Proposes a temporary (3-6 months) moratorium specifically on AI systems accessible by minors.

AI moratorium for minors

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Emphasizes demonstrable safety for children, strict content boundaries, validated safeguards, and the necessity of human oversight for AI interacting with children, particularly on sensitive topics.

we recommend that the guidelines further emphasise that AI systems must be designed and deployed in ways that are demonstrably safe for children.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Underscores special risks from AI systems like 'AI companions', calling for vigilance against threats such as deepfake creation and adverse impacts on minors' mental and physical health.

En outre, une attention particulière devrait être apportée au fonctionnement des systèmes d'Intelligence artificielle accessibles depuis la plateforme, en particulier en ce qui concerne les « IA Compagnions », compte tenu des risques que leur utilisation peut engendrer pour les droits des mineurs ainsi que pour leur santé mentale et physique.

Ten recommendations to the European Commission to really protect children online (unknown). Recommends mandatory safety requirements, independent oversight, and rigorous testing of AI tools accessible to minors to prevent behavioural risks and ensure explainability.

The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Promotes child

rights-focused AI design, stakeholder consultation (including children and experts), strict safeguards for sensitive topics, and consideration of children's evolving capacities.

We would recommend having a more comprehensive attention to the uptake of AI systems within online platforms accessible to minors and emphasise the need for platforms to design and deploy AI systems in a child rights conscious manner.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Advocates for EU Digital Services Act guidelines to feature enforceable requirements for the safe creation and deployment of AI tools used by minors, with oversight to ensure standards are met.

The guidelines should include specific requirements for the safe development, testing, and deployment of AI tools on platforms accessible to minors, along with independent oversight to verify compliance.

1.9.3 Transparency and Accountability

The category 'Transparency and Accountability' within AI and Automated System Governance for minors emphasizes the critical necessity for clear, accessible, and age-appropriate disclosures about the use of AI on digital platforms. Documents converge on the importance of robust labeling of AI-generated content and accounts, and advocate for real-time notifications that make it immediately apparent when minors are interacting with AI systems rather than humans. Several contributors stress that platforms must provide detailed explanations of AI functionality, offer straightforward opt-out mechanisms, and ensure transparency not only regarding the presence of AI but also concerning how training data and safety measures are employed. Protection of minors is a recurring theme, with guidelines recommending limitations or moratoria on certain AI features (such as chatbots/companions) for under-16 users and the provision of user-friendly information about AI processes. Further, there is an emphasis on the avoidance of emotionally manipulative design and minimizing data collection. Collectively, these insights argue for a proactive, comprehensive, and transparent approach, ensuring that children and their guardians can understand and actively manage their interactions with AI systems.

All implemented AI should be disclosed, and the mechanisms made as transparent as possible, particularly chatbots integrated into the services, along with their potential uses and functionality. (Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)))

Furthermore, there should be a mandatory labeling requirement not only for dedicated AI platform elements but also for users wishing to contribute AI generated content (including AI accounts) to the platform. (Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)))

Greece emphasizes the need to ensure that minors are explicitly informed when engaging with artificial intelligence rather than human actors. (Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Platforms should provide information on AI in a child-friendly and accessible way. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

It should be easy for users to switch off AI features and systems. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

This includes requiring clear disclosures, avoiding emotionally manipulative AI design, and offering easy opt-out mechanisms. (Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Comments on 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 (Federal

Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). This document highlights the need for AI transparency and security in relation to minors, proposing mandatory labeling of AI elements and clear disclosure of AI usage to protect young users.

All implemented AI should be disclosed, and the mechanisms made as transparent as possible, particularly chatbots integrated into the services, along with their potential uses and functionality.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). The submission calls for strict regulation, including a moratorium on AI chatbots or companions for under-16s, and demands public disclosure of AI training data and safety structures.

Immediate moratorium: No AI chatbots/companions for under-16s

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). The document advocates for transparency in AI deployment on platforms, easy opt-out options, and making AI-related information child-friendly and accessible.

Providers of online platforms should be transparent when Al is being used.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Similar to doc 72, this contribution urges for a ban on AI chatbot interactions for children under 16 and insists on transparent disclosure of training data and safety protocols.

Immediate moratorium: No AI chatbots/companions for under-16s

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 (European Commission). The guidelines propose technical solutions to warn minors when interacting with AI, ensuring clarity between AI and human interactions and emphasizing visibility throughout the interaction.

Ensure that if AI features and systems such as AI chatbots and filters are integrated into the service of an online platform, technical measures are implemented to warn minors that they are interacting with an AI system (60), that interactions with this system are different from human interactions and that these systems can provide information that is factually inaccurate and can 'hallucin

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Greece recommends making AI interactions truly transparent for minors with unambiguous disclosures, restrictions on manipulative design, and comprehensive information for both children and guardians.

Greece emphasizes the need to ensure that minors are explicitly informed when engaging with artificial intelligence rather than human actors.

1.9.4 Fairness and Bias Mitigation

AI and Automated System Governance in the area of Fairness and Bias Mitigation centers around ensuring that automated decisions and predictions are not discriminatory and remain transparent. Key insights emphasize the use of algorithms specifically designed to detect and mitigate bias within machine learning models. These practices are crucial in applications such as hiring, healthcare, credit scoring, and content recommendation. Best practices include regular audits of datasets and explicit documentation of bias mitigation efforts, especially for systems used by vulnerable populations like minors. The deployment of fairness toolkits and the transparent documentation of these processes are critical to fostering equitable AI outcomes.

Algorithmic Fairness Algorithms identify bias in machine learning models, preventing discrimination based on protected attributes. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

For example, IBM's AI Fairness 360 provides metrics and algorithms to assess discrimination and support adjustments, enabling transparent AI development. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

> *Dataset audits and bias mitigation strategies should be documented to avoid discriminatory effects.* (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))
>
> *Algorithmic Fairness Algorithms identify bias in machine learning models, preventing discrimination based on protected attributes.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))
>
> *For example, IBM's AI Fairness 360 provides metrics and algorithms to assess discrimination and support adjustments, enabling transparent AI development.* (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Highlights the importance of using specialized algorithms and toolkits to identify biases in AI models, ensuring transparency and fairness, particularly in high-stakes domains.

> *Algorithmic Fairness Algorithms identify bias in machine learning models, preventing discrimination based on protected attributes.*

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Stresses the necessity of documented audits and bias mitigation strategies, especially when algorithmic systems impact minors, to prevent discriminatory effects.

> *Dataset audits and bias mitigation strategies should be documented to avoid discriminatory effects.*

1.9.5 User Control and Safety

The collected insights under the category 'AI and Automated System Governance >> User Control and Safety' underscore a strong consensus on the urgent need for dedicated measures to protect children when engaging with AI systems, specifically chatbots and generative AI, on online platforms. There is a widespread call for comprehensive safeguards such as transparency requirements (explicitly notifying children when interacting with AI), prohibiting manipulative and human-like features that may blur the line between human and machine, and ensuring mechanisms for easy disengagement. These measures should also include restrictions on certain AI functionalities, such as avoiding unsolicited recommendations to children and limiting the topics AI tools can cover in conversations with minors. Several submissions highlight the necessity for guidelines to directly address the unique risks that AI chatbots pose to children's rights, privacy, and healthy development, separate from those applicable to the general user population. There is also recognition of the requirements for persistent warnings, age-appropriate explanations, opt-out options that do not impose financial burdens, and the broader integration of child safety by design in AI governance frameworks. Furthermore, some perspectives suggest balancing flexibility for providers in interface design with robust, protective standards for minors, and focusing on ethical AI design by reducing manipulative potential and encouraging human interaction where appropriate.

> *These should cover safeguards, transparency, prohibiting human-like features, avoiding being pushed or recommended to children and allowing the child to easily disengage from AI chatbots.* (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))
>
> *The guidelines should prohibit human-like AI targeting children, ban automatic promotion of such bots, require clear opt-out mechanisms, and set transparency.* (SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands))
>
> *Providers should be given flexibility to assess whether such a persistent warning is an "appropriate and proportionate measure" for the purposes of Article 28(1) DSA, bearing in mind the user interface, minor users' experience and the relative risks to the privacy, safety and security of minors resulting from the relevant AI systems.* (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))
>
> *These should cover safeguards, transparency, prohibiting human-like features, avoiding being pushed or recommended to children and allowing the child to easily disengage from AI chatbots.* (STATEMENT (Digipeace (Digirauha ry)))

Adopting these and other measures - on matters from recommender systems and governance to user support and reporting - may help providers of online platforms make online platforms safer, more secure and more privacy preserving for minors. (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 (European Commission))

This includes, but is not limited to, interactive or even gamified tutorials for child users, educational pop-up messages that surface throughout child users engagement, tips and reminders for children on how to stay safe online while using this service. (Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates for robust and tailored safeguards in AI systems interacting with children, emphasizing transparency and discouraging the sharing of sensitive information.

When considering AI chatbots, guidelines must include provisions to ensure not only transparency on the interaction with a machine, but on data use, preferably encouraging children not to share sensitive or personal information.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Calls for specific Digital Services Act guidelines to address AI chatbot risks for children, including dedicated safeguards, prohibition of human-like features, and ensuring children can easily disengage.

Given their increasing presence on online platforms and the significant risks they pose to children's rights and healthy development, they should be addressed separately with dedicated measures.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Recommends enforceable measures to prevent AI chatbots from emulating humans, making unsolicited recommendations, and simplifying disengagement for child users.

Given their increasing presence on online platforms and the significant risks they pose to children's rights and healthy development, they should be addressed separately with dedicated measures.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Highlights the unique risks from AI chatbots and digital companions, proposing bans on human-like AI targeting children, and requiring transparency and opt-out mechanisms.

The guidelines should prohibit human-like AI targeting children, ban automatic promotion of such bots, require clear opt-out mechanisms, and set transparency.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Emphasizes the need for separately addressed, AI-specific child protections including transparency, limits on human-like features, and means to avoid or disengage from AI chatbots.

These should cover safeguards, transparency, prohibiting human-like features, avoiding being pushed or recommended to children and allowing the child to easily disengage from AI chatbots.

STATEMENT (Digipeace (Digirauha ry)). Urges adoption of safeguards such as synthetic media labeling and age-appropriate AI content explanations to protect children online.

o age-appropriate explanations with regard to Al created content

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Suggests platforms limit the scope of AI conversations with minors (for example, avoiding medical advice) and monitor for manipulative or harmful interactions.

In addition to labelling AI interactions, platforms should limit the topics AI tools can discuss with minors (e.g., avoid medical or mental health advice) and apply monitoring to detect manipulation or harm.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Reiterates the necessity for child-specific safeguards against AI chatbot risks, demanding transparency, safe disengagement, and avoidance of harmful features.

Given their increasing presence on online platforms and the significant risks they pose to children's rights and healthy development, they should be addressed separately with dedicated measures.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recognizes the increasing presence of AI chatbots and the associated significant risks, advocating for dedicated protective measures for children's online experiences.

Given their increasing presence on online platforms and the significant risks they pose to children's rights and healthy development, they should be addressed separately with dedicated measures.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Advocates provider flexibility in applying persistent AI warnings for minors under the DSA, considering user experience and risk assessment.

Providers should be given flexibility to assess whether such a persistent warning is an "appropriate and proportionate measure" for the purposes of Article 28(1) DSA, bearing in mind the user interface, minor users' experience and the relative risks to the privacy, safety and security of minors resulting from the relevant AI systems.

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 (European Commission). Highlights the importance of adopting broad platform measures, including recommender system governance and robust user support, to improve minors' privacy and security.

Adopting these and other measures - on matters from recommender systems and governance to user support and reporting - may help providers of online platforms make online platforms safer, more secure and more privacy preserving for minors.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Proposes that AI chatbots should be off by default for minors, ensure no manipulative designs, and offer free, simple opt-out methods.

AI Chatbots should be disabled by default, not require payment to opt out of and be free of manipulative designs;

Joint Statement on Article 28 Guidelines (5Rights Foundation). Argues that existing guidelines fall short in protecting children from AI chatbot risks, advocating for specific and targeted mitigation features.

Given their increasing presence on online platforms and the significant risks they pose to children's rights and healthy development, they should be addressed separately with dedicated measures.

Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation). Welcomes acknowledgment of AI risks for children and calls for more detailed, dedicated regulatory guidance to protect child users.

The growing presence of artificial intelligence on platforms accessed by children demands dedicated attention.

The Case Against AI Simulated Empathy (unknown). Encourages ethical AI design that limits manipulative features, focuses on user guidance, and fosters human engagement, particularly to safeguard vulnerable users.

Instead, we should focus on ethical Al design-limiting manipulative tactics, encouraging human engagement, and providing clear user guidance.

1.9.6 Miscellaneous

1.10 User Empowerment, Agency, and Accessibility

The most compelling insight across these sub-categories is the insistence that digital environments for children move beyond mere protection and actively foster authentic empowerment, autonomy, and inclusivity. A foundational theme is that accessibility and inclusive design must be "a foundational principle, not a supplementary consideration," ensuring that all children—including those with disabilities or from marginalized backgrounds—can meaningfully engage with digital services. Multiple categories underline the importance of transparent, child-friendly communication: terms, policies, controls, and safety features should be delivered through clear language and a variety of modalities, with mechanisms in place to check real understanding and enable regular affirmation of choices. Giving children genuine control and personalization options—such as the ability to manage notifications, content feeds, and privacy settings—must be balanced carefully against manipulative design that could undermine agency. Participatory processes are strongly encouraged, with regular usability testing and user feedback incorporated into ongoing service improvements, especially for tools related to feedback, reporting, and support. Platforms are called to uphold children's full spectrum of rights online, including freedom of expression, information access, and the right to play, while ensuring healthy digital engagement via customizable tools that promote self-regulation and digital wellbeing. Across these threads, a clear consensus emerges: empowering children online means designing systems that respect their evolving capacities, honor their voices, accommodate diverse needs, and strike a critical balance between safety and agency.

1.10.1 Inclusive and Accessible Design

This set of insights collectively emphasizes the necessity for inclusive and accessible design in digital services aimed at children. Central to the recommendations is the explicit recognition of the diversity of children's needs, taking into account factors like age, disability, gender identity, migration status, socio-economic background, and family circumstances. Accessibility must be a foundational principle, not a supplementary consideration; all interfaces, information, and safety features should be intuitive, understandable, and usable by every child, including those with disabilities or additional accessibility needs. Moreover, the guidance stresses that communication should be child-friendly, with critical safety or privacy information presented using clear language, appropriate visuals, and multiple modes of delivery to maximize understanding and engagement. Inclusive processes should extend throughout the user journey, from registration and privacy settings to participation in reporting mechanisms and customization tools. Several documents call for active involvement and usability testing with children, especially those from marginalized and underserved groups, to ensure policies do not inadvertently exclude or disadvantage vulnerable youth. Lastly, the need for alternatives and fallback options for those lacking specific resources (such as digital devices or government IDs) is highlighted as vital to avoid new forms of digital exclusion.

> *Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;* (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown))

> *Ensuring that any tools, features, functionalities, settings, prompts, options and reporting, feedback and complaints mechanisms that are recommended in the present guidelines are child-friendly, age-appropriate, easy to find, access, understand and use for all minors, including those with disabilities and/or additional accessibility needs, and are easy to use and understand, and engaging, and do not require changing devices to complete any action involved.* (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 (European Commission))

> *The Commission encourages platforms to design their settings and user interfaces in ways that promote minors' digital autonomy, ensuring they are understandable and age-appropriate, including for children with disabilities.* (Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018))

> *Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed*

at them; (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

Providers should implement fallback options (e.g. local device checks, parental verification, or educational exemptions) for minors unable to use the primary AV/AE method. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

segregate-and-suppress laws "claim to protect children and teens, [but] they fail to truly consider the needs of the diverse and vast group of people they cover"). (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild advocates for accessible, inclusive, and child-friendly communication—especially in critical safety areas—ensuring children with disabilities or additional accessibility needs have equitable access to information.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document calls for explicit recognition of the varied and intersecting needs of children in all DSA-related measures, urging attention to accessibility and the diversity of children's lived experiences.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Bris emphasizes that all registration and information processes should be intuitive and accessible to users with diverse capacities and needs, with information accessible throughout the user journey.

To be effective, the registration process must be designed in a way that is intuitive and accessible to users with diverse capacities and needs.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). The Working Group on Gaming and Regulation encourages clearer definitions of accessibility terms and recommends involving children, including those with disabilities, in designing and evaluating services.

We also encourage the Commission to explain in more detail what is meant by terms such as 'child-friendly', 'age-appropriate', and 'easily accessible to all minors', including those with disabilities or additional accessibility needs.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Association e-Enfance/3018 stresses the need for understandable, age-appropriate interfaces and settings, and empowering minors' autonomy, including children with disabilities.

The Commission encourages platforms to design their settings and user interfaces in ways that promote minors' digital autonomy, ensuring they are understandable and age-appropriate, including for children with disabilities.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Missing Children Europe urges that the principle of acknowledging the diverse needs and backgrounds of children be embedded in the DSA guidelines, highlighting accessibility across all measures.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other

circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). This analysis warns of unintended exclusions caused by complex authentication processes and advocates for digital services that do not impose overbroad restrictions, recognizing the diverse needs and reactions of youth.

This claim may be a best-case scenario. A new Yoti user had to navigate 52 different steps to complete the authentication, a process that took over five minutes.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). SUPERRR Lab recommends centering the perspectives of marginalized and vulnerable users and calls for 'access by design' to be a central principle in digital regulation.

Currently, the framing of the guidelines places a strong emphasis on supporting providers to improve their services. While this is important, the perspective of users, especially those from marginalized and particularly vulnerable communities, should be the one that is centered throughout.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis calls for inclusive fallback mechanisms and accessible processes, warning that even privacy-preserving measures can create barriers for minors without adequate resources, thus emphasizing equitable digital participation.

Finally, even privacy-preserving age verification methods may create significant barriers for under served minors who lack access to smartphones, stable internet connectivity, or government- issued identification documents. Current guidance offers no substantive direction for developing inclusive alternatives that ensure equitable access to age-appropriate digital services regardless of socio-economic circumstances or technological access limitations. Addressing these accessibility concerns is essential for ensuring that protective measures do not inadvertently create new forms of digital exclusion for vulnerable young people who may already face significant barriers to digital participation.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document highlights the need for explicit recognition of children's varied needs and ensuring accessibility in all measures affecting them under the DSA.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). COFACE Families Europe advocates placing accessibility for all children, including those with disabilities or from disadvantaged backgrounds, as a general principle at the core of guidelines, ensuring information is universally available.

However, we suggest putting this as a general principle at the beginning of the guidelines and explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them.

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 (European Commission). The European Commission outlines the requirement that all tools, features, and communications for minors must be accessible, child-friendly, and easy to use for all, including those with additional needs.

Ensuring that any tools, features, functionalities, settings, prompts, options and reporting, feedback and complaints mechanisms that are recommended in the present guidelines are child-friendly, age-

appropriate, easy to find, access, understand and use for all minors, including those with disabilities and/or additional accessibility needs, and are easy to use and understand, and engaging, and do not require changing devices to complete any action involved.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). The Hellenic Ministry of Digital Governance stresses that registration processes should be easy to access and navigate for all minors, respecting their evolving capacities and accessibility needs.

Ensure that the registration process is easy for all minors to access and navigate depending on their evolving capacities ,including those with disabilities or additional accessibility needs.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). SIC DK recommends ensuring child-friendly, accessible language and processes in registration and account management, as well as educational initiatives framing such measures as protective.

We recommend that the Commission stress that registration processes should be communicated in child-friendly and easily understandable language, particularly in relation to age verification and protection from harmful content.

Protecting children online: response to the draft guidance (DIGITALEUROPE). DIGITALEUROPE supports inclusive access and rejects age-based bans, warning against national trends toward restricting digital participation for minors.

It is positive that the guidelines do not recommend age-based bans for children on social media. This is the correct approach.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document again reiterates the importance of recognizing the diversity of children's experiences and prioritizing accessibility in all DSA measures.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Save the Children argues for embedding principles that ensure the diversity of children's needs and accessibility at the heart of all guidelines, making measures more equitable.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

1.10.2 Transparency and Comprehension

The category 'Transparency and Comprehension' centers on ensuring that children and minors can clearly understand and interact with digital services in a way that respects their agency and safety. Across the documents, key recommendations include making terms and conditions, privacy policies, and platform functionalities accessible, age-appropriate, and communicated through multiple, child-friendly formats—not just text. There is strong emphasis on clear notification and explanation for changes (such as in terms or protective features), regular affirmation of choices, and mechanisms to check that minors truly comprehend what they are agreeing to. Specific strategies discussed include onboarding screens that prompt self-reflection, visual or gamified cues for explanations, comprehension checks via questionnaires, and simplified summaries or toolkits. Moreover, consideration is given to transparency regarding potentially confusing technology (such as explaining AI 'hallucinations'), and the need for clarity when legal protections change at adulthood. Additionally, documents highlight the importance of not overburdening minors or parents, ensuring they are not solely responsible for their safety, and including children's perspectives in service design.

Children's consent or assent should be meaningfully guaranteed regularly, especially when the terms of service change in a way that results in a use of data that the child did not consent to. (Eurochild

contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Amnesty International therefore recommends that the DSA Guidelines state that platforms should provide additional child-friendly non-textual means of communicating key aspects of a platform's terms and conditions on-platform, without requiring child users to search for such information. (SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International))

the contribution highlights the urgent need for age-appropriate, clear, and actively communicated terms. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

The Guidelines require that if AI features and systems are integrated into the service of an online platform, minors are warned "that they are interacting with an Al system, that interactions with this system are different from human interactions and that these systems can provide information that is factually inaccurate and can 'hallucinate". (Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE))

Communication strategies that clearly explain whether children are permitted to use specific services foster a sense of inclusion and agency in decision-making processes, allowing young people to understand and participate meaningfully in determinations that directly affect their digital experiences. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

line 482) ...functionalities allowing minors to decide how to engage with their services having, however, ensured that they are fully aware of this knowledge. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Advocates for ongoing, meaningful consent from children, especially when terms of service or data practices change, and emphasizes regular engagement to reaffirm or update their choices.

Children's consent or assent should be meaningfully guaranteed regularly, especially when the terms of service change in a way that results in a use of data that the child did not consent to.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Stresses that platforms must communicate terms and conditions through child-friendly and non-textual means to ensure comprehension without requiring children to actively search for information.

Amnesty International therefore recommends that the DSA Guidelines state that platforms should provide additional child-friendly non-textual means of communicating key aspects of a platform's terms and conditions on-platform, without requiring child users to search for such information.

Safe by Default (Panoptykon Foundation). Promotes the use of periodic onboarding screens to disrupt passive engagement and encourage intentional choices, supporting more reflective use by minors.

It would make the user stop and reflect 'what is my intention for this session?'.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Highlights the need to explain to minors what it means when AI systems 'hallucinate', promoting clear warnings about AI limitations and inaccuracies.

The Guidelines should explain what is meant by 'hallucinate' in this context.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Warns that critical information like terms and data practices are often inaccessible or unintelligible for younger users, calling for easily understandable communication.

Important information like terms of use, costs, or data collection practices are often hidden or hard to understand, which is especially problematic for younger users.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Recommends more practical guidance with examples, simplified summaries, user-friendly toolkits, and cautions against overloading children and parents with responsibility for privacy and safety.

Simplified toolkits would be helpful.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Suggests embedding transparency prompts that encourage minors to consult trusted adults in risky situations and calls for more child-informed and clear accessibility standards in service design.

In addition to the existing transparency recommendations, we suggest including prompts that actively encourage children to involve a parent or trusted adult before making decisions or taking actions that could pose a high risk to the

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Urges the development of age-appropriate explanation interfaces, using visual cues or gamified approaches, and transparent communication regarding children's service eligibility.

These might include visual cues, gamified interfaces, or contextual prompts, drawing from design research in the UK Children's Code and cognitive UX models from JRC and UNICEF.

Feedback DSA (unknown). Demands explicit, understandable notification for users turning 18 about the loss of child protections and introduction of adult features, with language tailored for children.

Clarify whether protections are gradually phased out or abruptly removed when a user turns 18. Platforms should: Notify users explicitly about the change

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Advocates for consistency between transparency design recommendations and established digital consumer protection principles, especially on dark patterns.

Align design recommendations with existing digital consumer protection principles, particularly regarding dark patterns, to ensure genuine user empowerment and informed choice.

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 (European Commission). Emphasizes drafting terms and explanations in ways minors can grasp, in line with regulatory transparency obligations and child-friendly communication of settings.

The Commission recalls the obligations related to terms and conditions set out in Article 14 of Regulation (EU) 2022/2065 and to transparency reporting provided in Article 15 of that Regulation for providers of intermediary services, which includes providers of online platforms;

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Calls for digital platforms to clearly and visibly disclose the lack of anonymity online to all users, including minors.

Elles doivent également faire figurer de manière parfaitement visible le fait qu'il n'existe pas d'anonymat sur internet.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Presses for actively communicated, clear, and tailored terms for minors, and the use of comprehension checks such as age-specific questionnaires before enabling engagement.

the contribution highlights the urgent need for age-appropriate, clear, and actively communicated terms.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Supports regular awareness and reminder strategies but cautions against overly frequent prompts that might unintentionally nudge users to alter safer settings.

For example, if a user has already chosen a more conservative setting, a "continuous" reminder of their settings choices could inadvertently encourage them to change it.

1.10.3 User Control and Personalization

The category 'User Control and Personalization' centers on empowering users—especially minors—with meaningful agency over their digital experiences. Across documents, there is a strong consensus on the importance of providing clear, accessible, and neutral mechanisms for users to personalize notifications, content, and privacy settings. This includes enabling children to choose the content and channels for receiving notifications, customize algorithmic feeds, and adjust account settings, always in ways appropriate to their age and evolving capacities. Genuine user choice is emphasized: platforms should avoid prescriptive defaults and 'friction' that deters user action, which can become 'dark patterns' that undermine the intent of user empowerment. A recurring theme is the need to protect minors from being nudged toward less protective settings, ensuring that their control over defaults is neither superficial nor subject to manipulative design. User-centric design principles advocate for flexibility, clear options, and age-appropriate controls that respect autonomy while safeguarding safety and privacy. Easy-to-use features for content/account deletion, muting, and personalization, as well as mechanisms to control or disable features like AI chatbots and tagging, are highlighted. Presenting choices at contextually relevant moments, rather than arbitrarily, is also encouraged to prevent confusion or fatigue. Ultimately, the documentation urges platforms and regulators to maximize agency and personalization without overwhelming or misleading users, establishing a fair and safe digital environment for all, particularly for minors.

measures that allow users to take control of their experiences online are crucial, particularly for minors. (CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe))

The guidelines should promote neutral design of online services and preserve genuine user choice, striking a balance between safeguarding minors and empowering users, including seamless usage of service. (CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)))

Make it easy and simple for minors to select which push notifications they get. (European Commission Article 28 Guidelines Feedback (unknown))

A case study examined by the Panoptykon Foundation demonstrates how Facebook uses algorithms to deliver personalized ads that may exploit users' mental vulnerabilities. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Maximizes human agency and control over user experience; designed to enhance social cohesion (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Instead of mandating rigid, feature or service level restrictions, platforms should be encouraged to provide clear, age-appropriate settings that allow users to manage content preferences, control the degree of personalization, and make informed decisions about the use of their data. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Emphasizes that children should be able to customize notification content, channels, and accounts according to their preferences, enhancing their sense of control.

Children should be enabled to choose the specific content, channels and accounts for which they receive notifications, when those notifications are turned on.

Salminen contribution protection of minors (Aalto University). Argues that user-facing controls—beyond algorithmic transparency—offer direct opportunities to improve children's well-being by allowing control over platform features and feeds.

Without diminishing the importance of algorithmic transparency and data privacy, the study argues that regulating these key risk features offers more immediate and impactful starting point for ensuring the well-being of children online.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Shows that lack of transparency and control over algorithms can expose users, including minors, to distressing content, highlighting the importance of meaningful content preferences and respecting user choices.

The study found Facebook's algorithms expose users to disturbing, trauma-related content despite their efforts to opt out, revealing that the platform does not give users meaningful control over what they see.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Stresses maximizing human agency by giving users explicit, respected choices over content, even if these choices contradict past engagement patterns.

Allow users to easily and explicitly indicate content they do or do not want, and respect users' explicit preferences even if contradicted by users' engagement.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Recommends robust user control options, particularly for minors, with a 'maximalist' approach to functionalities that underpin personal agency online.

measures that allow users to take control of their experiences online are crucial, particularly for minors.

Safe by Default (Panoptykon Foundation). Advocates for fairness and empowerment online, including through decentralized mechanisms and diverse content curation to bolster user choice.

Protecting fairness and consumer choice in a digital economy",

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Warns that prescriptive defaults and excessive friction in changing settings can constitute dark patterns and recommends neutral, easily changeable defaults for minors.

Prescriptive default settings and "friction" designed to deter users from certain actions risk being considered "dark patterns" under other DSA provisions (Recital 67).

CCIA Europe's Feedback to Public Consultation Guidelines for the protection of minors online under the Digital Services Act (DSA) (Computer & Communications Industry Association (CCIA Europe)). Calls for neutral design and genuine user choice, cautioning against default or interface manipulations that inhibit user empowerment—especially for minors.

The guidelines should promote neutral design of online services and preserve genuine user choice, striking a balance between safeguarding minors and empowering users, including seamless usage of service.

DOT Europe response1 (DOT Europe). Upholds the necessity for user agency in personalizing platform experiences and discourages constant consent-seeking or disregard for active user choices.

While we appreciate that default settings may play a big part in how users experience a service, it should be noted, however, that user agency is fundamental and that users should be able to design and personalise the service as best fits their needs.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Argues that minors must be able to easily delete content or accounts, supporting their right to privacy and control over their digital presence.

Implementing an easy to find and use function for deleting your own content and deleting the account as a whole.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Supports age-appropriate, autonomy-enhancing controls for minors and highlights concerns about user fatigue if controls are too burdensome or complex.

Importantly, the design of such controls must account for the risk of user fatigue.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Encourages neutral defaults in account settings to foster informed user choice for minors and avoids manipulative design patterns.

Prescriptive default settings and "friction" designed to deter users from certain actions risk being considered "dark patterns" under other DSA provisions (Recital 67).

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Urges clear delineation of which default settings minors should control, and prohibits design that nudges children toward weaker protections.

b) Default settings: clarify over which of the settings children should have control depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Recommends clarity in which controls children may adjust, always matching their evolving capacity and avoiding nudge techniques that reduce privacy or safety.

b) Default settings: clarify over which of the settings children should have control depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Calls for easy logout or profile deletion for minors and insists any shift from defaults must be opt-in, fully explained, and free from nudging.

Ensuring that minors can easily log out of services and delete their profiles and associated data provides young people with meaningful control over their digital presence and personal information.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Highlights alignment of control over default settings with children's evolving capacity and prevention of nudging towards less protection.

b) Default settings: clarify over which of the settings children should have control depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Supports clear and capacity-appropriate control over defaults for minors and underscores the avoidance of nudging towards reduced protection.

clarify over which of the settings children should have control depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

Feedback DSA (unknown). Proposes an opt-in option for users turning 18 to maintain heightened protections by choice.

Offer the option to maintain certain protections voluntarily.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Advocates for video auto-play being disabled by default to give minors proactive control over their viewing experience.

désactivation par défaut de la fonction de lecture automatique des vidéos

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Endorses an extensive set of functionalities empowering minors to control their engagement online, prioritizing agency and self-determination.

measures that allow users to take control of their experiences online are crucial, particularly for minors.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Warns that prescriptive defaults and extra friction may conflict with broader digital fairness principles and urges provision of robust user controls.

It is unclear how the proposed best practices mandating prescriptive default settings and requiring significant "friction" for any deviation are compatible with the provisions on online interface design and organisation in Article 25 DSA, the Unfair Commercial Practices Directive, or the data protection principles in the General Data Protection Regulation ("GDPR") (particularly the fairness and transparency principles in Article 5(1) GDPR).

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 (European Commission). Encourages implementing controls for minors such as blocking/muting, restricting comments, and customizing their interactions for safety and privacy.

The Commission considers that putting in place measures allowing minors to take control of their online experiences is an effective means of ensuring a high level of privacy, safety and security of minors for the purposes Article 28(1) of Regulation (EU) 2022/2065.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Stresses options for minors to disable AI chatbots, restrict tagging, and explicitly control features, avoiding nudging and ensuring user control.

Minors must have the options to disable or not see AI chatbots and should not be nudged towards using those features.

Joint Statement on Article 28 Guidelines (5Rights Foundation). Calls for clarity and protection in which platform settings children can control, guarding against design that promotes lowered protections.

b) Default settings: clarify over which of the settings children should have control depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Suggests that presenting user choices at contextually relevant times mitigates confusion, increasing likelihood of meaningful engagement with controls.

Empirical evidence suggests that choices should be presented at times when minors are most likely to consider them relevant.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Promotes a user-centric, flexible approach to control and personalization for minors, based on autonomy, proportionality, and inclusion.

This user-centric and flexible model, grounded in the principles of autonomy, proportionality, and inclusion, offers a more flexible and context-sensitive alternative to one-size-fits-all feature limitations, particularly given the diversity of developmental needs and digital literacy levels among children and young people.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Stresses clarification and safeguarding of children's control over platform defaults and prevention of nudging towards less privacy.

clarify over which of the settings children should have control depending on their evolving capacity and ensure that children are not nudged towards lowering their settings.

European Commission Article 28 Guidelines Feedback (unknown). Recommends that platforms make notification preferences easy for minors to control, emphasizing simplicity over complexity.

Make it easy and simple for minors to select which push notifications they get.

Consultation Response from Barnevakten, Norway - Regarding Article 28 of the EU Commission's Digital Services Act (DSA) (Barnevakten Foundation). Sets the basic expectation that children should be able to easily log out or delete accounts, supporting autonomy.

A basic requirement is that children must be able to easily log out or delete their accounts

1.10.4 Participation and Autonomy

The documents under 'Participation and Autonomy' in the broader context of user empowerment, agency, and accessibility emphasize the crucial importance of empowering minors—not simply protecting them—in digital environments. Key insights advocate for moving beyond restrictive or adult-centric frameworks, highlighting the necessity of fostering meaningful participation, autonomy, and informed decision-making among children and young people online. These contributions call for practical measures that enhance user control, such as tools for time management, consent mechanisms, and agency-respecting default settings; regular prompts to reinforce autonomy; and participatory, age-appropriate approaches reflected in regulatory design. Furthermore, the insights stress that children's rights in digital spaces are multi-faceted: in addition to safety, security, and privacy, well-being, flourishing, access to information, and inclusion are all vital. Stakeholders urge adopting evidence-based, balanced strategies that accommodate evolving capacities, allowing for graduated empowerment and the recognition that minors are active digital citizens. The ultimate objective is to create platforms and policies that support children and young people in exercising agency over their digital lives, making informed choices, and participating in ways that support their developmental needs and rights.

We also recommend strengthening the provisions of child participation and make it a general principle of the guidelines. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Here we suggest adding "These functionalities should provide the right balance between child agency and an adequate level of privacy, safety and security". (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))

Recognize the evolving capacities of minors and the importance of supporting their autonomy, safety, and access to information in parallel. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

Systems designed to be "good" may still centralize power and reduce user autonomy or informed consent. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Without such reminders, there is a risk that minors may become entrenched in narrow content loops or so-called "rabbit holes," shaped by prior engagement signals and algorithmic reinforcement. (Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår))

There should be in-application measurement of the mental state of the user. (European Commission Article 28 Guidelines Feedback (unknown))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Calls for designating time management and default setting changes as empowerment tools and recommends making child participation a foundational principle in DSA guidelines.

We also recommend strengthening the provisions of child participation and make it a general principle of the guidelines.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Highlights potential pitfalls in design aiming for 'goodness,' warning that such systems may still undermine user autonomy and meaningful consent.

Systems designed to be "good" may still centralize power and reduce user autonomy or informed consent.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). Advocates for an approach that evolves with children's age and needs, supporting inclusive participation and access rather than exclusion or excessive limitation.

Nous appelons donc à une approche équilibrée et évolutive, tenant compte des besoins, capacités et vulnérabilités des enfants selon les tranches d'âge, plutôt qu'une approche d'exclusion ou trop limitative, qui pourrait aller à l'encontre de leurs droits et de leur inclusion sociale.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Emphasizes balancing child agency and privacy, encouraging platforms to empower children's participation and well-being alongside safety and security.

Here we suggest adding "These functionalities should provide the right balance between child agency and an adequate level of privacy, safety and security".

Feedback DSA (unknown). Suggests shifting focus to not only protect but actively empower children and young people, maximizing positive impacts in digital environments.

Overall, there could perhaps be more focus on maximizing these positive effects, so that children and young people are not only protected but also empowered.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Recommends regular, age-appropriate reminders to enable children to manage and reconfigure their content choices, supporting autonomy and diverse experiences.

Periodic prompts can empower children to reassess and reconfigure their content preferences in line with their evolving needs and interests. This would strengthen children's autonomy and help ensure a more diverse and rights-respecting digital experience.

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 (European Commission). Stresses the importance of explicit notifications and affirmative choice in group participation to ensure minors' agency in digital interactions.

If the online platform offers group functions, ensure that minors join a group only after being notified of the invitation and upon accepting that they wish to be part of that group.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Promotes the use of choice screens as a mechanism to enhance user agency and foster competition within digital services.

Petrie, Gemma. "Beyond Choice Screens: Exploring browser choice screen interventions." Mozilla Foundation, 2024.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital

Services Act) (Snap). Urges recognition of minors' evolving capacities and supports the parallel development of autonomy, safety, and access to information.

Recognize the evolving capacities of minors and the importance of supporting their autonomy, safety, and access to information in parallel.

European Commission Article 28 Guidelines Feedback (unknown). Proposes that agency tools—such as self-set usage limits and in-app checks on well-being—should be made directly available to minors, measuring effectiveness from the user perspective.

Also, there should be a way for a teen to actually set real limits, for themselves, on their usage of the application (rather than requiring a guardian account to do it).

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Advocates for uniform, evidence-based measures going beyond content moderation, empowering children and parents to make informed digital choices.

1.10.5 Freedom of Expression and Rights

The documents in this category emphasize the imperative of upholding and explicitly safeguarding children's rights to freedom of expression and access to information in the digital environment. Multiple stakeholders urge regulatory guidelines under the Digital Services Act (DSA) to provide clear, explicit mention and robust protection of these rights, even as platforms are required to implement safety measures for minors. Representative insights highlight the importance of proportionality: privacy, dignity, the right to play, participation, and access to information must be balanced against safeguarding measures to prevent undue restriction of children's autonomy. Some contributors advocate for the recognition of emerging digital rights, such as digital dignity for minors, alongside traditional freedoms. Others warn that overly restrictive laws or segregated online spaces may unduly curtail minors' ability to participate in online forums and to seek content of their choosing—especially for marginalized youth who may find crucial community or identity support online. The overall consensus is that any restrictions or safeguards must be carefully balanced to preserve children's agency and voice online, considering the full spectrum of their rights enshrined in international conventions and charters.

The final guidelines should underscore the importance of safeguarding children's rights to freedom of expression and information when implementing any safeguards. (FEEDBACK: European Commission draft 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 (European Magazine Media Association (EMMA) and European Newspaper Publishers' Association (ENPA)))

Therefore, to ensure that measures to achieve a high level of privacy, safety and security for minors on an online platform are appropriate and proportionate, it is necessary to consider all children's rights, including their right to protection, non- discrimination, inclusion, participation, privacy, information and freedom of expression, among others. (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 (European Commission))

Children's rights form an integral part of human rights and all those rights are interrelated, interdependent and indivisible. (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 (European Commission))

This is a point of key importance, and we call for its explicit mention in the final guidelines with respect to any safeguards prescribed therein. (BDZV MVFP Reply to EC Art 28 DSA Draft Guidelines (BDZV Bundesverband Digitalpublisher und Zeitungsverleger e. V.; MVFP Medienverband der freien Presse e. V.))

However, accounts of minors should be discoverable to other minors, and accounts and content by adults should be allowed to be recommended to minors. (Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation))

As the Supreme Court indicated, "While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is

cyberspace-the 'vast democratic forums of the Internet' in general, and social media in particular." (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

BDZV MVFP Reply to EC Art 28 DSA Draft Guidelines (BDZV Bundesverband Digitalpublisher und Zeitungsverleger e. V.; MVFP Medienverband der freien Presse e. V.). Advocates for the explicit and repeated inclusion of children's rights to freedom of expression and information in DSA final guidelines as core principles when implementing safeguards.

Contribution Guidelines art 28 DSA (Respect Zone). Calls for the formal recognition of a right to digital dignity for minors as a guiding principle for all aspects of platform policy and design.

Respect Zone calls for the recognition of a fundamental right to digital dignity, especially for minors, to serve as a cross-cutting principle guiding platform design, moderation, recommendation systems, accessibility, and transparency.

Comments on the European Commission draft 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 ("DSA") (BDZV, MVFP). Underscores the need to protect children's rights to freedom of expression and information, calling for these rights to be explicitly addressed in all relevant guidelines and safeguards.

This is a point of key importance, and we call for its explicit mention in the final guidelines with respect to any safeguards prescribed therein.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Emphasizes that alongside protection, children's rights to play and participate must be considered in proportionality assessments when creating safety measures.

Nevertheless, the right to play (cf. Art. 31 of the Convention on the Rights of the Child) is not explicitly mentioned in the section "General Principles" (see p. 159 ff.) alongside "the right to protection, non-discrimination, inclusion, participation, privacy, information, and freedom

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Highlights the risk that restrictions targeting minors' online presence may undermine their First Amendment rights and exclude them from participating in vital digital forums.

Regulators should ensure that minors can raise their voices in the "most important places for the exchange of views."

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Points out that even with limits on recommendation systems, users—including minors—should always retain the ability to search for and access the content they choose.

Due to First Amendment considerations in the U.S., under both laws, there is a rule of construction that allows users to search for any content they would like to see.

FEEDBACK: European Commission draft 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 (European Magazine Media Association (EMMA) and European Newspaper Publishers' Association (ENPA)). Echoes the call for final guidelines to state unequivocally the importance of safeguarding children's rights to free expression and information within any safety framework.

The final guidelines should underscore the importance of safeguarding children's rights to freedom of expression and information when implementing any safeguards.

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 (European Commission). Reaffirms that all children's rights, including expression, information, participation, and privacy, must

be respected and are interrelated, interdependent, and indivisible when implementing online safety measures.

Therefore, to ensure that measures to achieve a high level of privacy, safety and security for minors on an online platform are appropriate and proportionate, it is necessary to consider all children's rights, including their right to protection, non- discrimination, inclusion, participation, privacy, information and freedom of expression, among others.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Warns that disproportionate safety measures might unduly restrict minors' access to supportive online spaces and opportunities for community, especially those from marginalized groups.

Especially for young people from marginalized communities, finding like minded people online can be crucial to establish a sense of identity and community.

1.10.6 Healthy Digital Engagement

The category of Healthy Digital Engagement within User Empowerment, Agency, and Accessibility focuses on enabling users—especially minors—to manage their time and engagement with online platforms in ways that promote digital wellbeing. Key insights from the documents center on the provision and systematic implementation of user-friendly, customizable time management tools, active session notifications, and positive nudges that foster self-awareness and self-regulation. There is a recurring emphasis on introducing 'friction' into digital experiences—such as limiting features, reminders, or altering display modes—to deter compulsive use, particularly where design patterns intentionally undermine user agency and promote addictive engagement. Additionally, the documents advocate for empowering minors with the ability to set content and time boundaries themselves, ensuring platform interfaces support healthy disengagement rather than maximize engagement metrics. Some submissions urge for healthy usage features to be adaptable and non-mandatory, arguing for contextually appropriate solutions across platforms. A notable trend is the call for more sophisticated interventions, such as digital nutrition scoring and time-aware algorithms, that assess and nudge usage towards healthier consumption patterns—complemented by clear guidance and positive nudges for safe, informed, and age-appropriate digital habits.

Introducing customisable, easy-to-use, child-friendly and effective time management tools to increase minors' awareness of their time spent on online platforms and help them engage with the service for no longer than they or their guardians intend. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Allow users to accessibly opt-out of revenue-maximizing design features (e.g., optimizing for time spent, infinite scroll, auto-play) that encourage greater usage. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

we recommend the systematic implementation of active notifications informing minors of the time spent online. (Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018))

Offer all users tools to limit their platform usage. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Tools must empower minors to implement both time-based and content-based boundaries, allowing for pre-commitment to avoiding addictive material or interaction types. (Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

We encourage the Commission to use clearer language to describe compulsive engagement and its relation to persuasive design patterns, which are often built into online environments, including games. (Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). This document recommends the introduction of customizable, child-friendly time management tools for minors that create real friction and offer nudges encouraging healthier engagement, such as time limits and low-stimulus display modes.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). The document highlights the importance of allowing users, particularly minors, to opt out of addictive design features and benefit from tools like digital nutrition scores and time-aware nudges that proactively promote healthy digital usage.

Allow users to accessibly opt-out of revenue-maximizing design features (e.g., optimizing for time spent, infinite scroll, auto-play) that encourage greater usage.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Emphasizing clarity in distinguishing user-driven versus design-driven excessive use, this document calls for guidance that underlines the value of positive nudges and measures to uphold user agency and the development of good digital habits.

It would be useful to clearly distinguish between 'excessive use' via the users own volition and design that intentionally undermines user agency.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). It advocates for systematic, active notifications that routinely inform minors of their online session duration, with the aim to raise screen-time awareness and encourage self-regulation.

we recommend the systematic implementation of active notifications informing minors of the time spent online.

Feedback DSA (unknown). The insight urges platforms to introduce time management tools that introduce friction such as pop-up warnings or feature restrictions following excessive use, targeting reduction of compulsive platform engagement.

Platforms should implement time management tools that introduce real friction to deter excessive use.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). The Greek submission calls for interface designs that discourage addictive engagement, empower minors to set time and content limits, and prioritize disengagement support over maximizing retention.

Interface success, it is argued, should be measured by its ability to protect and support minors’ disengagement, not to optimize engagement metrics.

Protecting children online: response to the draft guidance (DIGITALEUROPE). This response advises that healthy digital engagement features remain optional and context-sensitive, cautioning against rigid, prescriptive requirements that may not suit all platforms or age groups.

The guidelines rightly position these as optional features that support digital wellbeing, rather than mandated solutions.

1.10.7 Feedback, Reporting, and Support

The insights in the category 'User Empowerment, Agency, and Accessibility >> Feedback, Reporting, and Support' emphasize the centrality of easy-to-use, child-friendly feedback and reporting mechanisms as a foundation for the online protection and empowerment of minors. Across stakeholder feedback, there is broad consensus that all reporting, complaint, and redress tools must be designed to be accessible, intuitive, and understandable for children of various ages and abilities—including those with disabilities. Accessible support extends beyond reporting problems to also include providing timely, age-appropriate feedback about action taken and direct, clear avenues to support services and external assistance, like helplines and national Safer Internet Centres. There is also a strong focus on ensuring that children are not just able to report issues, but that these systems genuinely respond to their needs: platforms are urged to provide reasoned responses, make complaint outcomes transparent, and demonstrate that user feedback has tangible impact on algorithmic content delivery and platform moderation. Mechanisms for reporting should align with children’s language and comprehension levels, offer flexibility in how children can articulate their experiences, and support empowerment by reinforcing agency, privacy, and safety. Furthermore, several insights highlight the need for integrated support systems that do not leave children alone after reporting and encourage their involvement in ongoing design and review of these mechanisms.

online platforms should implement easily accessible feedback and reporting mechanisms that minors can use to report AI-generated content and responses they believe are not age-appropriate. (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 Feedback (Gesellschaft für Freiheitsrechte e.V.))

Effective user reporting - including from children themselves , feedback and complaints tools are essential for empowering children, and their parents/guardians, to notify online platforms about situations that may adversely affect children's privacy, safety and security. (Public consultation on 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 (Coimisiún na Meán))

Providing child-friendly and accessible feedback mechanisms supports children's sense of agency and autonomy in reporting as well as enhances control over their privacy and safety. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

There should also be an option available that allows minors to provide their own reasons for a report. (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 (European Commission))

The children and teenagers we accompany and who need assistance may find themselves in a state of distress, calling for rapid attention. (Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE))

Examples: Protection from inappropriate content, right to privacy, and freedom from digital bullying. (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Stresses the importance of online platforms providing minors with simple, accessible feedback and reporting tools to flag AI-generated or age-inappropriate content.

Public consultation on 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 (Coimisiún na Meán). Highlights the necessity for child-friendly, accessible reporting and complaints tools, including for children with disabilities, to empower children and families in safeguarding privacy and safety.

Effective user reporting - including from children themselves , feedback and complaints tools are essential for empowering children, and their parents/guardians, to notify online platforms about situations that may adversely affect children's privacy, safety and security.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Advocates for chatbots to incorporate easy-to-use, clearly understood reporting and feedback mechanisms tailored to children.

Chatbots should equally feature accessible and easy to understand reporting, feedback and complaints mechanisms.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Identifies gaps between risk assessment and child-focused redress, recommending that reporting systems address under-reporting and emerging harms with effective design and moderation.

This state of affairs poses the risk of under-reporting and allows emerging systemic risks to go undetected and further vulnerabilise children who are exposed to new harms.

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Examines children's experiences with blocking and reporting on social media and underscores the need to raise their awareness of online rights.

Blocking and Reporting: 70% of 7th graders have blocked someone online, but fewer have reported inappropriate content.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Emphasizes that accessible support services must be available for children who report violations so they receive societal and emotional assistance after reporting.

A critical aspect when children report violations is that they are not left alone in their situation.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Recommends that legal and external remedies from content moderation be tailored in format and accessibility for children and young people, ensuring age-friendly assistance.

It should be clarified that legal remedies and external assistance (e. g. as a result of moderation decisions), especially for children and young people, should be offered in a format and language appropriate for them and easily accessible.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Calls for providers to enable effective redress, not only reporting, especially allowing minors to correct mistaken age estimation and reverse unwanted purchases or decisions.

In addition to user reporting, providers should offer meaningful redress options for mistaken age estimation and for content or purchase regrets.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Advocates for reporting mechanisms that are specifically designed to be accessible and understandable for minors, with attention to language and ergonomics.

With regard to reporting systems, we strongly support the approach of ensuring that reporting mechanisms for minors are easily accessible and understandable.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Insists that, after submitting a report, children receive clear, age-appropriate information on any actions taken, highlighting the risk of eroding trust when responses are lacking.

After a report is made, children should be informed in accessible and age-appropriate language about what action was taken or is under consideration.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Supports meaningful redress options for children faced with incorrect age estimation or regretted content/purchase decisions, to increase their control online.

In addition to user reporting, providers should offer meaningful redress options for mistaken age estimation and for content or purchase regrets.

Protection of Minors Guidelines Response Request - Pursuant to Article 28 of the Digital Services Act (DSA) (Common Sense Media). Commends the focus on robust, child-friendly reporting and complaint tools that empower minors and guardians to address platform issues, citing comparable initiatives in the US.

The Commission has done a commendable job of identifying concerns with effective and child-friendly user reporting, feedback, and complaint tools that enable minors (and their guardians) to express and address issues with online platforms.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Underscores that child-friendly feedback tools enhance minors' agency, autonomy, and safety online, and endorses prioritizing accessibility and child-centric design.

Providing child-friendly and accessible feedback mechanisms supports children's sense of agency and autonomy in reporting as well as enhances control over their privacy and safety.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Welcomes provisions that mandate timely, comprehensible responses and support tool design that links minors to direct help and national support lines.

We welcome that each minor who submitted a report should be provided with a reasoned decision without undue delay, in a way that is adapted to the minor.

Microsoft response to the European Commission's draft 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 (Microsoft). Argues that, rather than expecting minors to justify reports, platforms should ensure reporting systems are easy to access and comprehend for children.

Rather, the focus should be on ensuring that reporting options are accessible and understandable to minors.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Suggests platforms should integrate prominent guidance to youth helplines and human support, especially as alternatives to automated assistance for minors.

Schließlich wäre noch auf die Integration von Hinweisen auf Hilfsangebote (Jugendberatungen, Online-Suchtstellen, Hotlines) im Nutzerbereich oder beim Überschreiten von Zeitlimits hinzuweisen.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Asserts the need for the reporting journey to be intuitive and user-centric, stressing clarity over arbitrary limits on steps required for minors to report.

We further note that there is no right amount of clicks a minor (or any other user) should go through to arrive at a reporting form. Rather, what is important is how clear, intuitive and user-friendly the overall user reporting journey is.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Promotes the availability of clearly visible information about helplines and support options for minors facing harmful or distressing online experiences.

Mögliche Maßnahmen: leicht auffindbare Hinweise zu Anlaufstellen oder Notrufnummern für Kinder und Jugendliche wie z. B. Rat auf Draht in Österreich.

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 (European Commission). Encourages platforms to let minors privately give varied feedback about online content and to adapt reporting options with customizable categories and free-text responses.

Allow minors to provide feedback about all content, activities, individuals, accounts or groups that they are shown on their accounts and that make them feel uncomfortable or that they want to see more or less of.

European Commission Consultation: Guidelines on the Protection of Minors Online Knight-Georgetown Institute (KGI) Response (Knight-Georgetown Institute). Urges that platforms be required to demonstrate that user feedback directly influences platform behavior and system outputs to enhance user agency.

The Commission should require platforms to demonstrate that user feedback does in fact have "lasting impact" on system outputs.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Supports guidelines for user reporting, complaint, and feedback tools that enable minors to effectively flag and resolve impacts on their privacy, safety, and security.

We support the Commissions guidelines for effective and child-friendly user reporting, feedback and complaint tools to enable minors to express and address features of online platforms that may negatively affect their privacy, safety and security.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Recommends that reporting mechanisms be child-friendly and that children's voices be involved in the design and evaluation of these tools.

In relation to reporting mechanisms, we consider crucial that they are child friendly to use.

1.10.8 Miscellaneous

1.11 Stakeholder Engagement and Child Participation

A defining insight across this category is that both stakeholder engagement and child participation must be substantive and deeply embedded across every stage of digital policy development and platform governance. Effective online child protection relies on involving a broad spectrum of voices—notably children themselves, alongside parents, experts, civil society, and survivor groups—in transparent, structured, and ongoing processes that shape the full lifecycle of safety policies and features. Children are recognized not just as vulnerable users but as rights holders and "key contributors" with unique perspectives, whose feedback often reveals risks adults might overlook. To avoid tokenism and guarantee legitimacy, mechanisms such as youth advisory boards, regulatory sandboxes, and regular feedback loops should be designed to reflect the diversity of children's backgrounds. Multiple sources emphasize that "stakeholders should influence the full lifecycle of platform governance," and that there must be clear documentation of how children's views directly shape outcomes, fostering trust and accountability. Inclusion of independent specialists and child rights experts is vital to ensure that consultation is both protective and effective, with policies tailored to the complexities of children's lived experiences. Overall, a consistent trend is the demand for regulatory mandates and institutional safeguards that center children's rights and perspectives in digital safety, supported by transparent, diverse, and non-tokenistic engagement mechanisms across all levels of governance.

1.11.1 Inclusive Stakeholder Engagement

Inclusive stakeholder engagement is consistently highlighted as critical for effective child protection online under the Digital Services Act (DSA) and related EU guidelines. Across documents, there is a strong consensus that platforms and policymakers must move beyond symbolic or minimal consultation; instead, they should establish transparent, structured, and meaningful mechanisms for the active participation of children, parents, experts, civil society, and human rights representatives. Stakeholders should influence the full lifecycle of platform governance, risk assessment, standard setting, and evaluation of safety measures. Cross-sector collaboration—including researchers and survivor groups—is emphasized, while multiple submissions point out gaps in current guidelines and urge the European Commission to mandate and document such cooperation to ensure that children's rights and experiences are central, not peripheral, to digital safety policies.

Incorporate parent, child, and expert input into platform governance, oversight boards, and evaluation cycles. (Policy_demands (unknown))

We therefore recommend emphasizing the importance of meaningful external stakeholder engagement, especially children as the affected rightsholders, in the process of both the identification and the mitigation of risks within the DSA Guidelines. (SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International))

COFACE strongly welcomes the need for regular consultations with minors, guardians and relevant stakeholders (line 953). (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

ountability: o Document how input influenced decisions (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))

d) Publicly document how stakeholder input has been incorporated into decisions, safety assessments, and updates to platform features or policies; (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures. (Ten recommendations to the European Commission to really protect children online (unknown))

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 Feedback (Gesellschaft für Freiheitsrechte e.V.). Highlights the necessity for mandatory cooperation and stakeholder involvement, especially independent experts and civil society, when developing age-appropriate content and risk reviews.

The Guidelines already acknowledge this in several places. However, this aspect should be strengthened, and mandatory cooperation should be required whenever criteria are being developed to determine what is age-appropriate or potentially harmful to minors.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Advocates for mechanisms ensuring parent, child, and expert input throughout platform governance, oversight, and evaluation, noting shortcomings in the current guidelines.

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Emphasizes the need for meaningful, not tokenistic, involvement of parents, children, and experts in digital platform governance and assessment processes.

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures.

Ten recommendations to the European Commission to really protect children online (unknown). Calls for integrating parent, child, and expert voices into the creation and evaluation of online platform regulations, to enhance the effectiveness of child protection efforts.

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Urges prioritizing meaningful external stakeholder engagement, particularly with children and other affected rightsholders, in the DSA's risk identification and mitigation processes.

We therefore recommend emphasizing the importance of meaningful external stakeholder engagement, especially children as the affected rightsholders, in the process of both the identification and the mitigation of risks within the DSA Guidelines.

CONCLUSION & POLICY DEMANDS (unknown). Identifies a critical gap in the guidelines: absence of mechanisms for substantial involvement of children and caregivers in shaping platform governance and safety evaluations.

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures.

Ten recommendations to the European Commission to really protect children online (unknown). Advocates for mandatory, significant participation of children, parents, and experts in the context of platform governance and evaluation under the DSA.

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures.

Policy_demands (unknown). Recommends requiring platforms to embed parent, child, and expert input into governance and oversight, highlighting the lack of effective mechanisms in current policies.

The guidelines refer to the importance of child rights but fail to establish a mechanism through which children and their caregivers are meaningfully involved in shaping platform governance or evaluating the success of safety measures.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Promotes the importance of cross-sector collaboration—particularly with researchers and civil society—in shaping safe and inclusive digital experiences for children.

Cross-sector collaboration, including researchers and civil society, is essential in developing safe and inclusive digital spaces for children.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Calls for mandatory stakeholder participation, with a focus on transparency about how stakeholder input influences decisions.

ountability: o Document how input influenced decisions

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Highlights the need for mandating stakeholder participation in decision-making, including documenting the impact of their input on final outcomes.

ountability: o Document how input influenced decisions

Welke rol kunnen Telecom bedrijven spelen in de bescherming van kinderen in de online wereld? (KidsUnplugged). Stresses the value of directly consulting parents to identify their priorities and needs concerning online child protection.

Bevraging aan ouders: wat willen ze en wat hebben ze nodig?

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Supports the necessity for regular, inclusive, and meaningful consultations with minors, guardians, and relevant stakeholders, warning against 'tick-the-box' exercises.

These consultations should be inclusive and meaningful, not just a tick-the-box exercise.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Recommends structured consultation with child protection organizations and survivors throughout the design and evaluation of online platforms.

Including structured stakeholder consultation with child protection organizations and survivors during both design and evaluation stages.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Proposes that platforms ensure stakeholder participation is mandated and that its influence is clearly documented for transparency.

ountability: o Document how input influenced decisions

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe (CDT Europe)). Draws attention to the underrepresentation of social science, human rights, and legal experts in standard setting, advocating for more diverse stakeholder inclusion.

However, a common issue is that standard setting organisations and their stakeholders often prioritize technical expertise, leading to underrepresentation of human rights, social science, and legal perspectives in standard development.

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 (European Commission). Encourages providers, regulators, researchers, and civil society to actively contribute to platform review processes impacting minors.

The Commission encourages providers of online platforms accessible to minors, Digital Services Coordinators, the research community and civil society organisations to contribute to this process.

Ten recommendations to the European Commission to really protect children online (unknown). Calls for platforms to not only acknowledge but operationalize mechanisms for parent and educator engagement, particularly structured feedback on changes influencing child monitoring and safety.

latforms must be required to: a) Engage with parents and educators in structured focus groups and feedback panels, especially when changes affect how guardians can monitor or support their children online.

1.11.2 Diverse and Meaningful Child Participation

The insights in this category stress that meaningful, diverse, and substantive child participation is essential for developing effective measures to ensure minors' privacy, safety, and security online. There is strong consensus across the documents that children's voices must be embedded not only in initial consultations but also in ongoing design, implementation, assessment, and revision of digital platforms and policies. Children are recognized as rights holders and key contributors, with a unique perspective on risks and safety measures, which often diverge from those of adults. Recommendations consistently emphasize structured mechanisms to include children from diverse backgrounds (considering age, gender, socio-economic status, etc.), to prevent tokenism and guarantee the effectiveness of their participation. This includes youth advisory boards, regular and systematic feedback loops, minor testing panels, regulatory sandboxes, and transparent methodologies for gathering and acting upon children's input. Furthermore, the documents highlight the importance of transparent processes demonstrating that children's views directly influence policy and product decisions, thus fostering trust and legitimacy. Beyond consultation, several documents call for an explicit regulatory mandate for substantive youth involvement in decision-making, with continued dialogue and direct engagement throughout the life cycle of online safety features. Diversity, inclusivity, and anti-tokenism measures are underscored as prerequisites for participation to genuinely reflect the lived realities of all children, especially those from structurally vulnerable groups.

This goes beyond consultation to include meaningful participation in decision-making processes, ensuring that children's lived experiences inform policy development and platform design. (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

Embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences; (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))

Platforms should conduct ethical testing of features using transparent methodologies and consult children meaningfully. (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))

Committees of young users designed to question the digital uses of young people, without imposing a precise agenda, but ensuring that a genuine and sincere voice emerges, firmly rooted in their own experiences. (Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE))

Although the framework appropriately encourages child participation in governance processes, it lacks essential guidance for ensuring ethical, inclusive, and meaningful engagement. (HOMO DIGITALIS

CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Collaborative approaches to child participation in design should be in line with international standards on children's rights to be heard and to participate in decisions affecting them, in particular the nine basic requirements for effective and ethical participation (Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild advocates for mainstreaming child participation throughout the Digital Services Act guidelines, with specific reference to involving children in assessing age assurance methods to address their real needs.

For assessing both the necessity and the appropriate age assurance method, it is crucial that children are directly involved to ensure it responds to their real needs and lived experiences.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Amnesty International highlights the need for children's ongoing involvement in implementing 'safety by design' on social media platforms, particularly in the development and monitoring of tools aimed at empowering young users.

Children and young people should also play a core part in implementing "safety by design" by being involved in the development and monitoring process of tools and features of social media platforms, especially where they are meant to meaningfully increase their agency and control.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). The UCD Centre for Digital Policy recommends mandating explicit, active, and substantive youth involvement in designing, implementing, and evaluating online safety measures, going beyond consultation to decision-making.

This goes beyond consultation to include meaningful participation in decision-making processes, ensuring that children's lived experiences inform policy development and platform design.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document calls for embedding child participation in the design and evaluation of all measures regarding minors' privacy, safety, and security, to ensure that these reflect children's lived experiences.

Embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences;

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Bris emphasizes prioritizing children's feedback within reporting and content moderation processes, recognizing that children's perceptions of online harm may differ from those of adults and can reveal unforeseen risks.

Children's feedback may reveal unforeseen and important risks related to privacy, safety and exposure to harmful content or online behaviour.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). EU Kids Online advises mandating platforms to meaningfully and transparently involve children and stakeholders in the evaluation and design of platform features, utilizing ethical testing and continuous feedback.

Platforms should conduct ethical testing of features using transparent methodologies and consult children meaningfully.

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 (BeSmartOnline! Maltese Safer Internet Centre). BeSmartOnline! Maltese Safer Internet Centre underlines the necessity of actively involving minors in shaping online safety tools and systems, recommending youth advisory boards for authentic insights into digital behaviors.

To ensure legitimacy and effectiveness, minors must be actively involved in shaping the tools and systems meant to protect them.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). INHOPE supports genuine and structured involvement of minors through ongoing dialogue and user committees that foster sincere, unscripted youth voices, contributing to democratic governance in digital policy.

The consultative nature of this kind of body would undoubtedly be the norm, but it would be useful to explore this subject in greater depth, particularly to serve the democratic aims of the European Union.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). 5Rights Foundation stresses embedding child participation in the design and evaluation of all protective digital measures, ensuring decisions are rooted in children's lived realities.

Embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences;

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Association e-Enfance/3018 recommends establishing minor testing panels and organizing regular consultations to gather and act on children’s experiences and suggestions before launching new features.

We support the establishment of minor testing panels across EU member states to assess the impact of new features before deployment.

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Defence for Children - ECPAT the Netherlands urges embedding inclusivity, diversity, and child participation as core DSA principles, ensuring structurally vulnerable groups are represented in safety measures.

Child participation: Throughout the development, review and evaluations of platform. Children must be meaningfully engaged in the development, testing and revision of all safety, privacy and security features, ensuring that these measures are grounded in their lived realities.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Missing Children Europe proposes that digital platforms be required to actively involve diverse children in developing and assessing reporting tools, with continuous feedback to ensure usability and trust.

Digital platforms should be required to actively involve children (including those with lived experience and from diverse backgrounds) in the development and assessment of reporting tools.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). This document critiques approaches that overlook youth perspectives in policy, instead advocating for the incorporation of young people's experiential knowledge into all digital safety policymaking.

Young people are active participants in their own online safety and have crucial insights into their own experiences and those of their peers. Their voices should be incorporated into policymaking discussions at every level");

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis points out that while child participation is encouraged, further guidance is needed to ensure ethical, inclusive, and meaningful engagement, including safeguards against tokenism and systematic feedback.

The current provisions do not address critical implementation considerations, including safeguards against tokenism, methodologies for ensuring diverse and representative child voices, and systematic feedback mechanisms that demonstrate how child input influences platform policies and practices.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document restates the imperative of embedding child participation in the development and evaluation of digital safety measures concerning minors' privacy, safety, and security.

Embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences;

Statement - DSA Guidelines (Protect Children). Protect Children argues for direct, ongoing involvement of children in designing and reassessing safety measures, recognizing the value of children's insights in creating responsive protection systems.

Involve children and young people directly in the design and continual reassessment of safety measures.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). COFACE Families Europe calls for embedding child participation in the design and evaluation of all online safety measures, grounding them in children's lived experiences.

embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences.

Joint Statement on Article 28 Guidelines (5Rights Foundation). 5Rights Foundation’s joint statement highlights the need to acknowledge the diversity of children’s experiences and embed their participation in shaping any measures that affect them.

Explicitly recognise the diversity of children's needs and their differing experiences based on their age, gender identity, sexual orientation, migration status, disability status, family type or any other circumstances or conditions, highlighting the importance of the accessibility of any measures directed at them;

Overall feedback on the Commissions guidelines on measures to ensure a high level of privacy, safety and security for minors online (ECPAT Sweden). ECPAT Sweden identifies the co-design of platform safety measures with children as vital, emphasizing that only children can accurately represent their digital realities.

It is therefore crucial that the platforms design their privacy, safety and security measures together with children, as it is the children themselves that have the best knowledge about their reality in the digital environment.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document echoes the call to embed child participation in all measures around privacy, safety, and security of minors, ensuring they represent lived experiences.

Embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences;

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Save the Children reiterates the importance of embedding child participation in the design and evaluation of privacy, safety, and security measures, informed by real experience.

Embed child participation in the design and evaluation of all measures that concern the privacy, safety and security of minors, ensuring that any measure is grounded and reflect their lived experiences;

Terre des Hommes submission to the DSA's article 28 draft guidelines open consultation (Terre des Hommes International Federation). Terre des Hommes International Federation promotes meaningful and regular consultation with children on platform design and transparency to ensure risks and solutions are identified by those most affected.

We welcome the guidance to regularly consult children on the design and evaluation of any elements of the platform that concern their privacy, safety and security, transparency requirements as well as testing and reviewing commercial communication with children.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Leiden Law School suggests making explicit the requirement to involve children and produce child-friendly impact assessments in DSA guidelines.

Additionally, a requirement for the involvement of children and child-friendly versions of impact assessments can be made explicit in the Guidelines.

1.11.3 Feedback and Consultation Mechanisms

The insights under 'Feedback and Consultation Mechanisms' stress the critical need for online platforms and regulators to establish structured, regular, and meaningful consultation with children, guardians, and other stakeholders regarding platform elements affecting minors' privacy, safety, and security. Stakeholder feedback—especially from minors—should not only be accommodated but prioritized and treated as a distinct category, recognizing that children's perceptions of harm often differ significantly from those of adults and may highlight unique or overlooked risks. Mechanisms should ensure that children are directly involved in the development, testing, and evaluation of these features, and that their input leads to concrete adjustments in moderation, recommender systems, and interface design. There is emphasis on the diversity and inclusivity of consulted minors, as well as the use of stakeholder dialogue to evaluate and adapt measures over time.

Regularly consulting with minors, guardians and relevant stakeholders on the design and evaluation of any elements of the platform that concern the privacy, safety and security of minors on the platform. (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 (European Commission))

The text should be strengthened to ensure that feedback from minors is not only accommodated, but actively prioritized. (The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government))

We therefore urge the Commission to recommend that online service providers are required to collect and analyse children's feedback separately from that of adults, to ensure that it is directly reflected in moderation and recommender system adaptations and to involve children meaningfully in the development and testing of these mechanisms. (Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår))

we recommend that the Commission strengthen the text to ensure that children's feedback is not only accommodated, but actively prioritised. (Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår))

e therefore urge the Commission to rec- ommend that providers of online platforms are required to collect and analyze children's feedback separately from that of adults as a distinct category. (The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government))

To contribute to non-discrimination and accessibility, providers should, where possible, involve in these consultations minors from a diverse range of cultural and linguistic backgrounds, of different ages, with disabilities and/or additional accessibility needs. (TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited))

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Recommends initiating a structured stakeholder dialogue one year after the DSA guidelines take effect to assess and adapt measures for protecting minors online.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Advocates for children's feedback to be actively prioritized and treated as a unique category in platform processes, reflecting their distinct experiences and risks.

We therefore urge the Commission to recommend that online service providers are required to collect and analyse children's feedback separately from that of adults, to ensure that it is directly reflected in moderation and recommender system adaptations and to involve children meaningfully in the development and testing of these mechanisms.

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 (European Commission). Calls for regular consultation and inclusive involvement of minors, guardians, and diverse stakeholders in designing and evaluating platform elements related to minors' privacy and safety.

Regularly consulting with minors, guardians and relevant stakeholders on the design and evaluation of any elements of the platform that concern the privacy, safety and security of minors on the platform.

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). Emphasizes active prioritization and separate analysis of feedback from minors, ensuring their input distinctly shapes moderation and design decisions.

The text should be strengthened to ensure that feedback from minors is not only accommodated, but actively prioritized.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Promotes ongoing consultation with minors and incorporation of their feedback into platform adjustments, considering broader changes in technology and user behavior.

Adjusting the design and functioning of the aforementioned elements based on the results of these consultations and on technical developments, research, changes in user behaviour or policy, product and usage evolutions, and changes to the harms and risks to the privacy, safety and security of minors on their platform.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Asserts that risk reviews should include consultations with children, guardians, and other stakeholders to better safeguard minors online.

We consider important for the risk review to entail a consultation process with children, guardians and relevant stakeholders.

1.11.4 Safeguards and Specialist Expertise

The key knowledge embedded in this category highlights the necessity of involving specialist expertise and establishing appropriate safeguards when engaging stakeholders and ensuring child participation in digital policy and governance. Insights emphasize that, to effectively integrate children's perspectives and protect their rights, it is important to consult child rights experts during procedural planning. The involvement of independent civil society and academic organizations—who offer in-depth understanding of children's rights, behavior, and development—can improve platform evaluation and help identify risks or barriers from a child-centered viewpoint. Finally, while engagement and participation of children in governance is essential for transparency and meaningful input, such involvement should be guided by specialist knowledge, recognizing that approaches must be nuanced and tailored, rather than generic.

engage with child rights experts locally in national enforcement planning. (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

We recommend that the guidelines explicitly encourage the involvement of independent civil society organisations and academic institutions in the testing and evaluation of platform systems, including through structured access to conduct external "stress tests." (Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår))

Whilst we support meaningful user engagement, the guidelines should acknowledge that engaging children in governance processes requires specialist knowledge and safeguards and should not be seen as a one-size-fits-all obligation. (Protecting children online: response to the draft guidance (DIGITALEUROPE))

engage with child rights experts locally in national enforcement planning. (UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

The guidelines also highlight the importance of transparency and participation, including engaging with children. (Protecting children online: response to the draft guidance (DIGITALEUROPE))

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Argues for the engagement of local child rights experts to inform national enforcement planning, ensuring that specialist perspectives guide decision-making.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Recommends structured involvement of independent civil society and academic organizations in platform testing and evaluation to bring expert, child-centered insights and strengthen safeguards.

We recommend that the guidelines explicitly encourage the involvement of independent civil society organisations and academic institutions in the testing and evaluation of platform systems, including through structured access to conduct external "stress tests."

Protecting children online: response to the draft guidance (DIGITALEUROPE). Highlights that children's participation in governance processes should be based on specialized expertise and robust safeguards, recognizing that engagement must be context-sensitive and not standardized.

Whilst we support meaningful user engagement, the guidelines should acknowledge that engaging children in governance processes requires specialist knowledge and safeguards and should not be seen as a one-size-fits-all obligation.

1.11.5 Governance and Oversight

The key insights in the category 'Stakeholder Engagement and Child Participation >> Governance and Oversight' emphasize the importance of inclusive governance structures in online child protection. Effective oversight requires the active involvement of a diverse range of stakeholders, notably including children, parents, experts, and civil society, in the creation, revision, and evaluation of online safety policies and platform governance. Multistakeholder groups are recommended for drafting and refining guidelines, while structured processes for input from children and their caregivers are necessary to ensure that governance mechanisms truly reflect the needs and rights of young users. Transparency is also highlighted through the call to publicly document how stakeholder input affects safety assessments and platform updates.

The Commission should establish a multi-stakeholder group to revise and improve the draft, including existing national regulators, private sector age assurance providers, and civil society. (Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association))

Incorporate parent, child, and expert input into platform governance, oversight boards, and evaluation cycles. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

tion policy review processes. c) Consult with children and young people on platform design, safety tools, and policy changes, using age-appropriate participatory methods (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Incorporate parent, child, and expert input into platform governance, oversight boards, and evaluation cycles. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

tion policy review processes. c) Consult with children and young people on platform design, safety tools, and policy changes, using age-appropriate participatory methods (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Detailed Feedback on Article 28 DSA Guidelines for the Protection of Minors (Age Verification Providers Association). This document advocates for the formation of a multi-stakeholder group, including national regulators, private sector actors, and civil society, to collaboratively improve draft guidelines for protecting minors online.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). This document recommends meaningful and structured engagement of parents, children, experts, and civil society in platform governance, with processes to solicit and incorporate diverse feedback in safety policy design and revision.

Incorporate parent, child, and expert input into platform governance, oversight boards, and evaluation cycles.

1.11.6 Miscellaneous

1.12 Education, Awareness, and Digital Literacy

A central insight across education, awareness, and digital literacy is that prevention, empowerment, and resilience-building—rather than restrictiveness—form the foundation of effective digital safety for young people. Coordinated efforts spanning formal education, family engagement, and industry partnerships drive this approach, as “parents, educators, industry, policymakers, and community organizations should work together as a 'village' to guide, support, and empower young people.” School-based digital literacy is most impactful when it is comprehensive, age-appropriate, and consistently updated to address emerging online risks, incorporating themes like digital rights, ethical data use, privacy, and media literacy. Successful strategies include mandatory digital literacy curriculum elements, accessible parental resources, targeted awareness campaigns, and transparent, scenario-based tutorials on platforms. These initiatives are enhanced by ongoing evaluation, national alignment, and active input from children, parents, and industry. Ethical considerations—such as responsible AI engagement and data transparency—are increasingly relevant, while the integration of digital education with technological safeguards ensures all users can benefit from privacy and security measures. Collectively, these trends show that digital literacy is most effective when inclusive, collaborative, and adaptive, bridging the gaps between knowledge, practical skills, ethical judgment, and safe participation in digital environments.

1.12.1 Formal and School-Based Digital Literacy

Formal and school-based digital literacy initiatives across Europe consistently emphasize the importance of comprehensive, structured digital education for both minors and their guardians. Key knowledge in this category centers on integrating digital literacy, media competence, and awareness about online risks as mandatory elements within school curricula, starting from the earliest digital interactions. Numerous contributions recommend a minimum digital age of majority (e.g., 15 years old), call for guidelines that strengthen children's agency through digital literacy, and promote digital responsibility and safe behaviors online. A recurring insight is that prevention and empowerment must be prioritized over paternalistic or restrictive measures, with young people guided to develop resilience, decision-making skills, and critical evaluation of online environments. Effective approaches include explicit training on digital rights, privacy, consumer protection, and the identification of harmful behaviors such as problematic gaming, gambling, or addiction. These initiatives advocate for age-appropriate materials, interactive formats, parental and teacher support, and collaboration with NGOs and industry to create adaptive, accessible educational content. The contributions also highlight the value of school-based interventions in reducing risky behaviors and fostering a balanced use of digital media. Platforms, regulatory bodies, and educators are urged to invest in media literacy tools and awareness campaigns, and to ensure that guidance is proactive, inclusive, and tailored to evolving digital risks.

This should be accompanied by a robust educational strategy, empowering and involving young people in digital responsibility. (Contribution Guidelines art 28 DSA (Respect Zone))

regulators should move "beyond a narrow focus on preventing harm through bans and restrictions, towards empowering young people with the knowledge, resilience, and support they need to navigate the digital world safely"); (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Homo Digitalis firmly believes that minors must receive structured education on digital rights, consumer protection, and children's rights throughout primary and secondary schooling. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Adolescents' social media use should be preceded by training in social media literacy to ensure that users have developed psychologically-informed competencies and skills that will maximize the chances for balanced, safe, and meaningful social media use."). (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

The classroom intervention through the activities in the eduCAC teaching unit led to a reduction in the intensity and frequency of video game use. (What do you bet? (Que t'hi jugues) (Catalan Audiovisual Council (CAC)))

regulators should move "beyond a narrow focus on preventing harm through bans and restrictions, towards empowering young people with the knowledge, resilience, and support they need to navigate the digital world safely"); (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Contribution Guidelines art 28 DSA (Respect Zone). Recommends the establishment of a European digital age of majority at 15, mandating digital education and active NGO involvement from the earliest point of digital engagement.

Digital education must be made mandatory from the first point of digital engagement, with NGOs actively involved in designing preventive and educational content tailored to different age groups.

Public consultation on 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 (Coimisiún na Meán). Argues for stronger media literacy recommendations in EU guidelines to empower children and parents, including action plans by platforms and improved understanding of digital safety tools.

An Coimisiun recommends that the narrative running through the draft guidelines in relation to children's agency and empowerment can be strengthened further by introducing explicit recommendations in relation to media literacy, particularly for children and their parents/guardians.

What do you bet? (Que t'hi jugues) (Catalan Audiovisual Council (CAC)). Demonstrates the impact of classroom interventions on reducing problematic video game use and enhancing students' ability to identify gambling-related risks, supported by comprehensive teaching resources.

Before the intervention, 24.1% of students played video games 5-7 days a week. After the intervention, this percentage fell to 4.2%. This finding confirms that the teaching unit has a positive effect on prevention.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Critiques restrictive online measures for minors and advocates for digital/social media literacy training that empowers adolescents to navigate online risks independently and thoughtfully.

As one child said, "Kids don't need protection we need guidance. If you protect us you are making us weaker we don't go through all the trial and error necessary to learn what we need to survive on our own ... don't fight our battles for us just give us assistance when we need it."

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Stresses the need for comprehensive digital literacy education about digital rights, consumer protection, and children's rights throughout primary and secondary schooling.

Homo Digitalis firmly believes that minors must receive structured education on digital rights, consumer protection, and children's rights throughout primary and secondary schooling.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). Highlights media literacy as essential for protecting young people online, with examples of industry-led educational initiatives promoting responsible online behavior.

Additionally, we wish to highlight the importance of fostering media literacy among young people in ensuring their protection online.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Calls for systematic media literacy promotion and awareness about digital addiction, encouraging self-regulation and providing age-appropriate resources for both youth and guardians.

Kinder und Jugendliche durch Bildung befähigt werden müssen, Risiken im digitalen Raum zu erkennen und zu vermeiden, etwa in Bezug auf Datenschutz, Betrug, Cybermobbing oder radikale Inhalte.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Emphasizes the requirement for media literacy measures and awareness-raising tools for minors, endorsing skills that help them navigate and seek necessary support online.

Finally, the Media Board highlights the importance of media literacy measures and tools, that VSPs have to put in place and the awareness raising about those tools.

1.12.2 Family and Community Engagement

The category of Family and Community Engagement within Education, Awareness, and Digital Literacy centers on the importance of a holistic and collaborative approach to promoting digital literacy and online safety for children. Instead of relying on restrictive or fear-based policies, the insights emphasize that parents, educators, industry, policymakers, and community organizations should work together as a 'village' to guide, support, and empower young people. This involves providing ongoing education to both children and parents so that families feel equipped to foster resilience, autonomy, and responsible digital citizenship. There is also a recognition that parents often require tailored resources, training, and community support, as the rapid evolution of digital technology can leave them feeling unprepared for the challenges their children face online. The importance of broad-based, multi-stakeholder initiatives such as public awareness campaigns and partnerships with family and media literacy organizations is highlighted, with efforts focused on informing and engaging parents in meaningful conversations with their children. Practical recommendations include creating accessible resources, national helplines, and topic-specific guidance, ensuring families have the tools and ongoing support necessary for safeguarding children's online experience and personal growth.

addressing health, safety, and privacy concerns for youth online must involve an on-going, whole-of-society approach in which industry, parents and caregivers, schools, health providers, other community-based organizations, and policymakers play their roles"); (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

we call on a whole village of parents, caregivers, researchers, technology designers/developers, clinicians, educators, and policymakers to put efforts toward positive media parenting and resilience-based approaches to promote the digital well-being of adolescents"). (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

The video game industry has launched public awareness campaigns in 16 countries in local languages to inform parents about PEGI and the tools they have access to in order to set fair rules, but importantly to also inform parents on how to start a dialogue and how to take an interest in their children's online activities (Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI))

Digital Literacy and Citizenship Education for Children. When minors mature into adults, they will need digital expertise to navigate social situations and succeed in the labor market. (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Instead of abruptly granting access to new services at a specific age, a more effective approach involves providing supportive tools for children to build resilience and navigate online services safely (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

Train Parents to Become Better Teachers. As the expression goes, parents are their children's first teachers. (The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown))

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). This document emphasizes the necessity of involving all stakeholders—parents, educators, industry, and policymakers—in teaching digital literacy and online resilience, advocating collaborative family-based strategies over restrictive measures that may hinder children's development.

addressing health, safety, and privacy concerns for youth online must involve an on-going, whole-of-society approach in which industry, parents and caregivers, schools, health providers, other community-based organizations, and policymakers play their roles");

Microsoft response to the European Commission's draft 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 (Microsoft). This document suggests the creation and aggregation of national support resources and topic guidance to help families navigate online safety and privacy challenges more effectively.

To support implementation, the Commission may wish to aggregate an up-to-date list of national helplines and other support services, including guidance on the topics where each has capability.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). This document highlights the value of public awareness initiatives and partnerships to increase parental engagement and knowledge regarding digital safety tools, promoting dialogue and interest in children's online activities.

The video game industry has launched public awareness campaigns in 16 countries in local languages to inform parents about PEGI and the tools they have access to in order to set fair rules, but importantly to also inform parents on how to start a dialogue and how to take an interest in their children's online activities

1.12.3 Awareness Campaigns and Training

The insights in the category 'Awareness Campaigns and Training' emphasize the multifaceted approach needed to enhance online safety, privacy, and security for minors. Key recommendations across documents highlight the importance of implementing effective media literacy and cybersecurity training, targeting not only young users themselves but also those responsible for their care and online environments, such as developers, moderators, and complaint teams. There is a clear call for awareness-raising campaigns, education, and prevention efforts to be benchmarked and evaluated for impact to ensure their effectiveness. Additionally, several contributions underscore the value of clear communication strategies and the acknowledgement of industry-led initiatives—such as influencer training in advertising standards—to broaden the reach and legitimacy of awareness efforts. The documents also suggest expanding the scope of training to various relevant groups in the digital ecosystem, and recommend national and European alignment in both policy and practice, leveraging initiatives like the Better Internet for Kids strategy and Safer Internet Centres.

the Media Board highlights the importance of media literacy measures and tools, that VSPs have to put in place and the awareness raising about those tools. (Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services))

To ensure the effectiveness of awareness-raising efforts, we recommend defining benchmarks and encouraging impact evaluation. (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))

This approach is in line with the Better Internet for Kids strategy (BIK+), which emphasises the importance of awareness and education in promoting online safety and supports the implementation of Regulation (EU) 2022/2065 in this respect. (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 (European Commission))

For example, the German SRO has designed an influencer training course – a voluntary offering, covering legal duties, proper disclosure, and responsible advertising. (AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)))

ensuring the privacy, safety, and security of children and adolescents requires a comprehensive approach that includes both technical and non- technical tools. (Guidelines to ensure high levels of privacy, safety, and security for minors online (Kaspersky))

Providing persons responsible for minors' privacy, safety and security, developers, persons in charge of moderation and/or those receiving reports or complaints from minors, with relevant training and information (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 (European Commission))

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). This document stresses the significance of media literacy measures and awareness campaigns, emphasizing that video-sharing platforms (VSPs) should promote tools and guidance for minors navigating their services.

the Media Board highlights the importance of media literacy measures and tools, that VSPs have to put in place and the awareness raising about those tools.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). It calls for clarification and the establishment of benchmarks to evaluate and improve the effectiveness of awareness-raising activities targeting the protection of minors online.

To ensure the effectiveness of awareness-raising efforts, we recommend defining benchmarks and encouraging impact evaluation.

Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act Allwyn submission (Allwyn). The submission advocates for targeted education and prevention campaigns directed at underage users as a way to bolster online safety.

Education and prevention campaigns.

Welke rol kunnen Telecom bedrijven spelen in de bescherming van kinderen in de online wereld? (KidsUnplugged). The insight recommends that telecom companies should communicate proactively about child protection strategies and screen use guidelines in their communications.

Communiceer actief in eigen communicatie over het beschermen van kinderen, over de richtlijnen van de Franse expertencommissie rond schermgebruik1 en hoe een startphone veel problemen kan vermijde

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). This document encourages the recognition and uptake of voluntary influencer training courses developed by self-regulatory organizations, underlining their growing adoption across EU member states.

The work in this space has been intensifying with other SROs in different EU Member States currently in the process of launching similar training, under the umbrella of the European Advertising Standards Alliance (EASA).

Guidelines to ensure high levels of privacy, safety, and security for minors online (Kaspersky). It suggests incorporating Cybersecurity Literacy Trainings into the core set of protective measures for platforms accessible to minors and offering practical tools like privacy checkers.

the set of core measures outlined in the guidelines could be expanded to include a new category: "Cybersecurity Literacy Trainings."

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 (European Commission). The guidelines advocate for comprehensive awareness and educational initiatives, including specialized training for those directly responsible for minors' safety online.

This approach is in line with the Better Internet for Kids strategy (BIK+), which emphasises the importance of awareness and education in promoting online safety and supports the implementation of Regulation (EU) 2022/2065 in this respect.

Mitteilung der Bundesregierung der Bundesrepublik Deutschland an die Europäische Kommission (Bundesregierung der Bundesrepublik Deutschland). This submission urges expanding training obligations to encompass diverse roles, such as complaint teams, chat moderators, and IT staff, for a thorough protection scheme.

Es wird empfohlen die in den Leitlinien angesprochenen Schulungen auf weitere Gruppen wie Beschwerdeteams, Chat-Moderatorinnen und IT-Mitarbeitenden zu erweitern.

1.12.4 Media, Information, and Data Ethics

The category 'Media, Information, and Data Ethics' encompasses foundational knowledge about digital literacy, emphasizing transparency, empowerment, and ethical considerations in how individuals, especially children, engage with digital platforms and data-driven technologies. Key insights include recognizing the importance of data ethics as data becomes pervasive in daily life, understanding digital business models (such as targeted advertising), and acknowledging disparities in digital knowledge across age groups and genders. Furthermore, digital literacy must address not only technical comprehension (like algorithms and cookies) but also foster critical thinking about privacy, online boundaries, and responsible AI use. The rise of AI-driven interactions introduces new ethical concerns, such as the risk of over-reliance on simulated empathy, which necessitates educating users on maintaining healthy boundaries with technology.

> *Data Ethics: Increasingly important as data becomes integral to daily life.* (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))
>
> *For example , if you search for dresses, your Facebook can see that , and then it shows you advertisements for what you have searched for .* (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))
>
> *Education on healthy boundaries with technology can mitigate over- reliance, rather than banning AI empathy outrigh* (The Case Against AI Simulated Empathy (unknown))
>
> *7th Graders: 13% understand algorithms, 53% understand cookies.* (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))
>
> *4th Graders: Only 1% understand algorithms, 15% understand cookies.* (CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår))
>
> *Education on healthy boundaries with technology can mitigate over- reliance, rather than banning AI empathy outrigh* (The Case Against AI Simulated Empathy (unknown))
>
> **CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår).** This document highlights children's varying degrees of understanding about data collection and algorithmic processes, emphasizing the need for education on digital business models and data ethics in alignment with transparency and empowerment principles. It also points to notable age and gender gaps in digital literacy among schoolchildren.
>
> *For example , if you search for dresses, your Facebook can see that , and then it shows you advertisements for what you have searched for .*
>
> **The Case Against AI Simulated Empathy (unknown).** This document argues for the importance of educating users about the boundaries and ethical considerations of interacting with AI, particularly concerning the risks of over-dependence on simulated AI empathy. It suggests that responsible digital literacy should focus on user empowerment rather than technological prohibition.
>
> *Education on healthy boundaries with technology can mitigate over- reliance, rather than banning AI empathy outrigh*

1.12.5 Platform Tools and Safety Features

The insights in this category highlight the importance of accessible, effective, and proactive education on platform tools and safety features for both minors and their guardians. Central recommendations include integrating digital literacy and safety tutorials—preferably interactive and mandatory—into onboarding and registration processes, ensuring tutorials and information are revisitable and updated, and using child-friendly communication methods such as audiovisual content and bite-sized direct messaging across time. Platforms are urged to regularly inform minors and caregivers about privacy, safety, and security features, as well as platform functionalities, using language and formats suitable for young users. There is a strong emphasis on proactive support, helping children understand risks, rules of conduct, and available resources before harm occurs or problems are reported, with particular attention to risks like addiction, mental health, and privacy implications. Notably, these insights stress the responsibility of platforms to empower both children and guardians through clear instructions, scenario-based education, and transparency about tools and their limitations. They advocate for ongoing, iterative improvement in communication styles to match minors' comprehension needs, and for the promotion of digital agency and resilience, addressing not just risks but fostering positive engagement with technology.

Caregivers often find it difficult to engage with parental controls or other tools at their disposal to support children's experiences online. Since platforms are the best placed to do this as designers of such tools, they should provide accessible information about the caregivers' role and the tools they can use to support children's safety and privacy online. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

We therefore propose that platforms should implement child-friendly interactive tutorials that guide users through platform interfaces and safety features, followed by practical assessments that allow minors to demonstrate their understanding of safe platform usage.
(UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy))

Provide information to minors and, where relevant, their guardians, about any measures put in place to ensure a high level of privacy, safety or security of minors on the platform. (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 (European Commission))

Because minors are unlikely to dig into the transparency policy on platforms, such as the terms of service or security options, we highly recommended that the Commission encourage platforms to supply information to minors over time. (II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute))

Platforms can proactively support children through in-app guidance, digital literacy prompts, and scenario-based education on what to do when facing harm. (HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis))

Les plateformes de jeux vidéos, en particulier, doivent diffuser de manière régulière des messages d'avertissement contre les risques d'addiction, et suggérer des temps de pause à intervalles réguliers. (Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Encourages platforms to provide digital literacy tools and accessible online safety education to guardians, enabling them to better support minors' safety and privacy online.

Caregivers often find it difficult to engage with parental controls or other tools at their disposal to support children's experiences online. Since platforms are the best placed to do this as designers of such tools, they should provide accessible information about the caregivers' role and the tools they can use to support children's safety and privacy online.

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Recommends providers raise awareness of privacy and safety tools for children using child-friendly, non-textual methods on a regular basis.

Finally, providers should regularly raise awareness in child-friendly ways, including through non-textual means, of the available privacy and safety-related user tools.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Proposes the implementation of child-friendly, interactive safety tutorials and practical assessments during registration, ensuring minors understand safety features and can exercise their rights effectively.

We therefore propose that platforms should implement child-friendly interactive tutorials that guide users through platform interfaces and safety features, followed by practical assessments that allow minors to demonstrate their understanding of safe platform usage.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Advocates for delivering information to minors in short, direct bursts across multiple sessions to increase awareness and comprehension of available safety tools, with continuous improvement of communication methods.

Short bursts of direct information over multiple sessions could result in higher comprehension and awareness of the tools available to minors.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Calls for proactive platform support using in-app guidance, digital literacy prompts, and scenario-based education to build digital resilience in children before issues occur.

Platforms can proactively support children through in-app guidance, digital literacy prompts, and scenario-based education on what to do when facing harm.

Feedback DSA (unknown). Supports the idea of mandatory and revisitable onboarding safety tutorials (like 'NiceSpace') to build minors' digital literacy, safety awareness, and informed agency on platforms.

The “NiceSpace” interactive tutorial is an excellent model.

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 (European Commission). Highlights the need to provide age-appropriate and accessible information to minors and guardians about privacy, safety, security, and platform functionalities in compliance with EU law.

Provide information to minors and, where relevant, their guardians, about any measures put in place to ensure a high level of privacy, safety or security of minors on the platform.

Consultation sur les lignes directrices relatives à la protection des mineurs en ligne au titre de la législation sur les services numériques (art. 28 du DSA) (Commission Nationale Consultative des Droits de l'Homme (CNCDH)). Emphasizes regularly communicating safety and addiction risks to minors and guardians, including concrete recommendations and warnings in accessible language.

Les plateformes doivent communiquer auprès des mineurs et de leurs parents, dans un langage facile à lire et à comprendre, sur les différents types de risques auxquels sont exposés les mineurs en ligne (cf. la typologie des risques « 5C » élaborée par l'OCDE).

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Suggests using the registration process as a prime opportunity to educate minors on safety features, rules of conduct, risks, and available supports in ways that are both understandable and effectively discouraging risky behavior.

Use the registration process as one of the main opportunities to highlight the safety features of the platform or service, the rules of conduct along with their respective consequences for violating terms, any identified risks to a minor’s privacy, mental health, safety or security and resources available to support users as well as in a way that is understandable and at the same time discouraging for minors (audiovisual materials, pop up, etc).

1.12.6 Miscellaneous

This category emphasizes the importance of integrating educational initiatives with technological safeguards to ensure effective digital literacy and awareness, particularly concerning online privacy, safety, and security for minors. It highlights the need for solutions that adhere to privacy laws, protect fundamental rights, and are both practical for businesses and accessible to users. The knowledge embedded here advocates for a balanced approach that combines robust technology with education, empowering users to adopt and correctly utilize digital solutions in a rapidly evolving online environment.

we believe we are in a unique position to inform the EC of the facts we can share relating to the issues pertinent to EC's considerations and offer useful information and guidance on solutions that align with applicable privacy laws, protect citizens' fundamental rights, are feasible to implement for legitimate businesses across the Union, and combine robust technological measures with education to ensure they are properly adopted and used correctly. (CONTRIBUTION TO THE EUROPEAN COMMISSION - DG CNECT - CNECT F2 In the matter of "Consultation" on 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 (WebGroup Czech Republic, a.s.))

1.13 Enforcement, Accountability, and Legal Compliance

Across all sub-categories, a unified call emerges for transparency, specificity, and enforceability in how the Digital Services Act (DSA) safeguards minors online. The most compelling insight is the consensus that effective accountability and compliance require not only clear legal boundaries but also mandatory, harmonized enforcement—"compliance with regulations... must not be voluntary." Success hinges on lucid alignment of the DSA with both national and sectoral laws to avoid duplication and fragmentation, ensured by transparent regulatory scopes and clarification of the guidelines' legal status. Effective governance is highlighted through proposals for coordinated and clearly defined roles for authorities and platforms, including sufficient resources for Digital Services Coordinators and clear mandates for all involved bodies. Procedural clarity is underscored by calls for detailed, regularly reviewed processes, from enforcement readiness and complaint systems to audit standards and structured redress mechanisms—including "creating real personal (civil and criminal) liability for public or platform decision-makers in cases of gross negligence." Proportionality, support, and guidance remain crucial: most contributions emphasize non-binding, adaptable guidelines that avoid excessive burdens for smaller providers, backed by practical examples, grace periods, and support mechanisms. With regular, independent audits and outcome-based assessments, enforcement is urged to be both effective and fair. Synthesizing these themes, the dominant trend is the push toward accountability measures that are not just robust in principle but operational, pragmatic, and coordinated, with a strong focus on harmonization and child-centered protection.

1.13.1 Legal Scope and Regulatory Alignment

The documents under the category 'Legal Scope and Regulatory Alignment' articulate the necessity for the Digital Services Act (DSA) guidelines—especially those concerning the protection of minors—to be clearly scoped, harmonized, and aligned with existing EU and national laws. A resounding theme is the call for the guidelines to avoid duplication, overreach, or conflict with sector-specific, national, or parallel EU regulations (such as the Audiovisual Media Services Directive, GDPR, or forthcoming laws). Stakeholders advocate for the legal boundaries and interplay between the DSA and other frameworks to be transparently clarified, with a focus on maintaining the DSA's harmonizing intent and preventing fragmentation of the Digital Single Market. Contributors highlight the importance of expressly delimiting the applicability of the guidelines—restricting them to platforms and services defined by the DSA, and not inadvertently expanding their scope to unrelated services (e.g., editorial media, VoD, or VLOSEs). Many urge the Commission to detail the legal status and enforceability of the guidelines, recommend referencing or integrating pre-existing sectoral obligations, and emphasize subsidiarity and national competence where appropriate (such as in gambling or implementation of age verification). Interesting discussions include proposals to treat online platforms and e-commerce sites equivalently to brick-and-mortar establishments regarding restricted goods, to clarify the conditions for compliance with emerging technologies like blockchain, and to ensure researchers' safe harbor under platform terms when probing for vulnerabilities—all within the evolving legal landscape shaped by the DSA.

> *Bereits in ihrer Stellungnahme aus September 2024 betonten die Medienanstalten, dass angesichts des Anwendungsbereichs der Leitlinien unbedingt gewährleistet sein sollte, dass bestehende rechtlich bindende Regelungen der Richtlinie 2010/13/EU (Richtli- nie über audiovisuelle Mediendienste - AVMD-RL) maßgeblich be- rücksichtigt werden müss* (Art. 28 DSA Leitlinien Stellungnahme der Medienanstalten (Medienanstalten))

> *In alignment with the DSA's goal to harmonise regulatory approaches across the EU and prevent conflicting laws, we urge the Commission to clarify that Article 28 and the corresponding Guidelines are the mechanisms through which online platforms should fulfill their obligations to protect minors online in the European Union.* (Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company))

> *We consider that the guidelines include relevant references in relation to the DSA (for instance when they refer to the functionality required by the Article 26(2) and therefore, similarly they could include references to the obligations of the AVMSD (and in particular, its Article 28b).* (Public consultation on 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 (Coimisiún na Meán))

> *Rather than seeking to render blockchain technologies incompatible with GDPR, the objective should be to clarify the conditions under which their design and operation can be aligned with the Regulation.* (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

This includes recognising that legal obligations and public interest objectives (notably, traceability; compliance; and fraud prevention) may justify the persistence of certain data in a secure, decentralised, and transparent way. (Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan))

Expressly underline DSA supremacy over national law (Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.))

BDZV MVFP Reply to EC Art 28 DSA Draft Guidelines (BDZV Bundesverband Digitalpublisher und Zeitungsverleger e. V.; MVFP Medienverband der freien Presse e. V.). Advocates for the exclusion of editorial online platforms from the scope of Article 28(4) DSA guidelines, arguing these platforms already have sufficient safeguards and do not pose significant risks to minors.

Contribution Guidelines art 28 DSA (Respect Zone). Recommends extending DSA guidelines to include intermediate-size platforms and generative AI tools, highlighting the need for clear regulatory scope over emerging digital services.

These guidelines should also apply to intermediate-size platforms widely used by minors (such as Discord or Twitch), and to generative AI tools.

Public consultation on 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 (Coimisiún na Meán). Emphasizes the complementarity between the DSA and AVMSD in minors' protection and calls for platforms' terms and conditions to reflect existing legal obligations across EU frameworks.

An Coimisiun suggests that the guidelines could include a more prominent reference on the complementarity of their framework, when it comes to minor's protection, with the media content rules of the AVMSD (Article 28b in particular).

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Stresses that DSA guidelines should explicitly affirm the supremacy of DSA provisions over conflicting national laws for harmonized enforcement.

Expressly underline DSA supremacy over national law

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). Suggests that online e-commerce sites be regulated in a manner similar to physical stores regarding access to restricted products, aligning digital and offline legal requirements.

nline e-commerce sites should be treated and regulated similarly to brick-and-mortar stores, and "access" to restricted products should refer to the checkout or delivery stage (depending on applicable national or EU laws)

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). Proposes clarifying how blockchain operations can be lawfully aligned with regulations, recognizing specific legal and public interest justifications for data persistence.

This includes recognising that legal obligations and public interest objectives (notably, traceability; compliance; and fraud prevention) may justify the persistence of certain data in a secure, decentralised, and transparent way.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Argues for the enforcement of safe harbor protections for researchers, noting current legal barriers imposed by platform terms that deter critical safety research.

Despite digital platforms and AI companies' commitments to encourage third-party discovery of issues, many impose barriers that deter safety research.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Requests clearer articulation of the DSA's scope and its relationship with other EU regulations, particularly concerning age assurance and the definition of 'highest standards'.

As such any proposed measure in the Draft Guidelines needs to be for specifying Art. 28 para. 1 DSA, and not another DSA article, or aspect of regulation.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). Asks the Commission to clarify the legal applicability and expectations of the guidelines for Very Large Online Platforms and Search Engines (VLOP/VLOSE) under the DSA.

Nous appelons enfin la Commission à mieux expliciter la portée juridique des lignes directrices pour les VLOP (Very Large Online Platforms - très grandes plateformes en ligne) et les VLOSE (Very Large Online Search Engines - très grands moteurs de recherche en ligne).

ACT RESPONSE TO THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Association of Commercial Television and Video on Demand in Europe (ACT)). Urges that guidelines' scope remains limited to platforms covered under the DSA and not be extended to video-on-demand services, citing differing regulatory structures.

ACT calls on the Commission to ensure that the guidelines are not viewed as a universal standard for protecting minors online and that their scope remains limited to platforms regulated under the DSA.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Insists that the guidelines should only apply to Online Platforms as per DSA definitions, and proposes deleting or modifying sections unrelated to this scope.

The draft Guidelines are properly scoped to Online Platforms, as defined in Article 3 of the DSA.

Amazon's contribution to the Guidelines on the protection of minors under Article 28 of the Digital Services Act (DSA) (Amazon). Highlights the need to clarify that the guidelines do not expand the DSA's scope or incorporate previously excluded features, maintaining legal precision.

However, Section 6.1.2 should be clarified so that the Guidelines' suggestion to implement mitigations at the feature level does not inadvertently imply that the scope of the DSA extends to such features if they were previously outside the scope of the DSA.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Warns against reinterpreting established legal concepts of 'purchase' and 'contract' within the DSA guidelines and suggests alignment with current law and co-/self-regulatory practices.

re-interpret long-standing legal concepts of what constitutes a "purchase", and therefore a "contract" under EU law, which are matters that should not be re-interpreted within the scope of the DSA, and particularly not without a robust study having been first conducted regarding the economic impact that such a fundamental re-interpretation of existing EU law would have on Europe's digital single market.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Recommends explicit referencing of AVMSD and relevant national laws for harmonised minor protection and effective implementation for video-sharing platforms.

An explicit reference both the AVMSD and to such relevant national laws could allow a coordinated and comprehensive approach to minor protection.

DOT Europe response1 (DOT Europe). Emphasizes harmonised EU-wide enforcement of the DSA, cautioning against diverging national rules that could undermine regulatory consistency.

Moreover, we encourage policymakers to keep the focus on harmonisation of the regulatory framework through the DSA, to ensure a coherent and consistent application of the rules at EU and national levels to all online platforms.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Suggests clarifying that guidelines are not directly applicable to VLOSEs due to their unique nature and the specific scope of Article 28 DSA.

It should be clarified that for Very Large Online Search Engines (VLOSEs), the guidelines may be inspirational, but not directly relevant both due to the scope of Article 28 DSA and the fundamentally different nature of search engine services.

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Calls for equal regulatory treatment between online and offline e-commerce actors to prevent unfair legal disparities.

E-commerce actors should not be treated or regulated differently than brick and mortar ones.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Advocates for clarification on the legal weight of proposed measures and a presumption of compliance for platforms fully implementing the guidelines, to ensure transparency and investment certainty.

foster broad and effective adoption of the guidelines, we encourage the Commission to: · Clarify the legal weight of the proposed measures: establishing a presumption of compliance for platforms that fully implement the guidelines would be a powerful lever for trust.

The European Lotteries' Response to Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act (The European Lotteries). Supports the guidelines' respect for national competence and the subsidiarity principle, particularly regarding national gambling regulations under the DSA.

EL welcomes the Commission's decision to develop guidelines, as this instrument appropriately takes into account the subsidiarity principle.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Advises against adopting regulatory frameworks proven unconstitutional in other contexts (such as the U.S. CDA and COPA) for child online safety in the EU.

This is essentially the regulatory approach Congress took in both the 1990s-era Communications Decency Act (CDA) and Child Online Protection Act (COPA), both of which ultimately were deemed unconstitutional.

Art. 28 DSA Leitlinien Stellungnahme der Medienanstalten (Medienanstalten). Stresses the importance of considering pre-existing binding regulations and clarifying the non-binding nature of the DSA guidelines within national contexts.

Bereits in ihrer Stellungnahme aus September 2024 betonten die Medienanstalten, dass angesichts des Anwendungsbereichs der Leitlinien unbedingt gewährleistet sein sollte, dass bestehende rechtlich bindende Regelungen der Richtlinie 2010/13/EU (Richtli- nie über audiovisuelle Mediendienste - AVMD-RL) maßgeblich be- rücksichtigt werden müss

Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance). Points out inconsistencies in defining minors across EU laws and urges harmonization and clear delineation to avoid compliance confusion under the DSA.

We note an inconsistency between the draft Guidelines' concept of a minor as under 18 years of age and other legislative texts, such as the General Data Protection Regulation (GDPR), which sets the age of digital consent between 13 and 16 depending on the Member State.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families

Europe). Promotes emphasizing corporate responsibility to respect human rights, including children's and disability rights, as a general DSA principle.

Businesses have a corporate responsibility to respect human rights, including children's rights and the rights of people with disabilities.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). Highlights the necessity for legislative coherence between the DSA, AVMSD, and upcoming frameworks (like the Digital Fairness Act) to avoid ambiguity and business burdens.

Lastly, we wish to highlight the need for the final guidelines to have due regard to upcoming legislative initiatives such as the review of the Audiovisual Media Services Directive (AVMSD), which is due by the end of 2026, as well as the Digital Fairness Act (DFA) and the Consumer Protection Agenda to ensure legal coherence.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Advocates for coordination of DSA guidelines with sectoral regulations (audiovisual, data protection, consumer rights, AI) in minors' protection.

L'Arcom note que plusieurs acteurs de la société civile et du monde de la recherche ont appelé son attention sur la nécessité d'une bonne articulation des lignes directrices avec les régulations sectorielles relatives à la protection des mineurs (i.e. droit de l'audiovisuel - plateformes de partage de vidéos -, droit des consommateurs, droit des données personnelles, régulation de l'intelligence artificielle).

FEEDBACK: European Commission draft 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 (European Magazine Media Association (EMMA) and European Newspaper Publishers' Association (ENPA)). Requests explicit exclusion of editorial platforms from further DSA measures due to their minimal risk to minors and existing editorial safeguards.

In light of the negligible or non-existent risk to minors posed by these editorial platforms and given the already considerable burden of implementing the DSA obligations for these offerings, we call on the Commission to explicitly exclude them from requirements to implement additional measures prescribed in the guidelines.

Comments of Slovak DSC to the EC Guidelines on Protection of Minors (Slovak Digital Skills Coalition). Proposes adding clarifications on the interplay between the DSA and the AVMSD within the guidelines for greater legal certainty.

As established by the Digital Services Act (DSA), this regulation applies independently and in parallel with Directive 2010/13/EU, clarifying and supplementing it where relevant through horizontal rules.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Recommends a comprehensive list of relevant EU child protection laws and initiatives, with special emphasis on national legal differences.

Ergänzungsvorschlag BMASGPK: Vollständige Auflistung von EU Jugendschutzbestimmungen und -initiativen. Einleitender prominenter Hinweis, dass Jugendschutz in den nationalen Rechtsordnungen der 27 EU-MS unterschiedlich geregelt ist.

Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology). Argues that ongoing and forthcoming legislation should not delay timely and comprehensive action for children's rights within the DSA framework.

Neither the existence of other EU legislative instruments nor the possible adoption of announced legislative initiatives, such as the Digital Fairness Act, should serve as a pretext to delay necessary and

comprehensive action for the realisation of children's rights in the context of the Digital Services Act, which, together with other applicable EU rules, engages the protections enshrined in the Charter of Fundamental Rights of the European Union.

Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry). Warns against guidelines that extend, duplicate, or conflict with DSA's structured provisions and insists on delineating DSA from other EU obligations.

It must be ensured that the guidelines do not disproportionately extend or duplicate the measures for minors' safety provided for in Article 28 of the DSA and the complementary risk-based obligations set out in Articles 34 and following of the DSA.

EL PAPEL DEL ENTORNO DIGITAL EN LA NORMALIZACIÓN DE LOS NUEVOS PRODUCTOS DE TABACO Y NICOTINA (Asociación Española Contra el Cáncer). Calls for the withdrawal of regulatory exemptions for heated tobacco products, ensuring alignment with EU directives.

Directiva Delegada (UE) 2022/2100 de la Comisión, de 29 de junio de 2022, por la que se modifica la Directiva 2014/40/UE en lo que respecta a la retirada de determinadas excepciones aplicables a los productos de tabaco calentado.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Seeks clarity on when DSA Article 28(1) takes precedence over national laws and guidance, referencing the intent to harmonize intermediary services rules EU-wide.

We would welcome clarity from the Commission on the circumstances in which Article 28(1) DSA pre-empts national laws transposing EU legislation and national guidance on the protection of minors, bearing in mind the aim of the DSA to harmonise rules on the provision of intermediary services (Article 1(2) DSA), particularly in relation to "issues on which [EU] legal acts leave Member States the possibility of adopting certain measures at national level" (Recital 10), as is the case with e.g. Article 28b(1)(a) AVMS Directive.

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 (European Commission). Notes the Commission's obligation to assess and report by 2025 on how the DSA interrelates with other legal acts.

Under Article 91 of Regulation (EU) 2022/2065, the Commission is mandated to evaluate and report, by 17th November 2025, on the way that this Regulation interacts with other legal acts, in particular the acts referred to above.

Position of Polish Confederation Lewiatan on Commission’s consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan). Warns of national initiatives undermining harmonized DSA provisions and fragmentation risks in the Digital Single Market.

Recently, a number of national initiatives have sought to disrupt the consistent application of harmonized rules established by the DSA, including on protection of minors online.

Middle Tech Europe response to the draft guidelines under Article 28 DSA (Middle Tech Europe). Requests reassurance that the guideline measures constitute a non-exhaustive list and cautions against embedding forthcoming laws into current DSA guidance.

We strongly caution against anticipating the DFA by embedding its forthcoming rules into today's DSA guidance.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). Urges comprehensive referencing of sector-specific obligations for VSPs under AVMSD within the DSA guidelines for consistency and compliance.

However, with this contribution we encourage the Commission to add all the individual reference to sector specific obligations related to VSPs, instead of referencing only some of them in the footnotes17:

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Recommends aligning guidelines with GDPR, international frameworks (e.g., UNCRC), and national child protection measures to ensure clarity and avoid duplication.

Alignment with Existing Frameworks: The guidelines should continue to align with the GDPR, internationally recognised frameworks on Children's rights such as the United Nations Convention on the Rights of the Child (UNCRC), and national child protection measures to avoid duplication and ensure legal clarity.

Response to the consultation on the European Commission's draft 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 (LinkedIn Ireland Unlimited Company). Advocates that Article 28 and the related guidelines should be the primary mechanism for platforms' obligations, streamlining compliance and avoiding regulatory duplication.

In alignment with the DSA's goal to harmonise regulatory approaches across the EU and prevent conflicting laws, we urge the Commission to clarify that Article 28 and the corresponding Guidelines are the mechanisms through which online platforms should fulfill their obligations to protect minors online in the European Union.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Urges avoidance of prescriptive, duplicative, or conflicting requirements within the DSA that overlap with existing EU legislation.

Avoid prescriptive requirements that duplicate or conflict with existing EU legislation on data protection, commercial practices, and consumer rights;

Protecting children online: response to the draft guidance (DIGITALEUROPE). Calls for clearer guidance on the interface between the DSA and EU legislation such as the AVMSD, GDPR, and the eIDAS framework.

However, the guidelines should go further in clarifying the relationship between the DSA and other EU legislation, including the Audiovisual Media Services Directive (AVMSD), the General Data Protection Regulation (GDPR), and the upcoming eIDAS framework.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Highlights that many DSA guideline requirements duplicate existing EU law and warns that excessive guidance may lead to confusion.

As such, these requirements are already sufficiently addressed and further guidance risks creating unnecessary confusion.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Argues that national laws on legal capacity should be considered in determining platforms' obligations for lawful contracting and data processing under DSA.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Seeks clearer explanation of how the DSA guidelines interact with existing EU and national legislation, emphasizing that they should not override sectoral laws.

This stated, it is important to clarify that the "Guidelines" do not override national and sectorial regulations in existing areas.

Feedback on the guidelines on protection of minors online under the Digital Services Act (unknown). Recommends explicit citation of additional articles relevant to minors in the DSA and clearer differentiation between legal and policy guidelines.

The Digital Services Act has thus far clearly differentiated between legal and policy infringement.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). Suggests that DSA guidelines should reference industry codes of conduct for practices not directly covered by law, like virtual currencies and random rewards.

The PEGI Code of Conduct addresses these practices specifically (see paragraph 8 below).

Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency). Notes that many DSA guideline recommendations overlap existing Union legislation and calls for their removal to prevent enforcement confusion.

Hence, the Swedish Consumer Agency considers that such recommendations should be removed from the guidance to avoid creating overlaps in terms of enforcement, and confusion on applicable law and guidance.

1.13.2 Roles, Responsibilities, and Coordination

This category focuses on defining and coordinating roles, responsibilities, and mechanisms for effective enforcement, accountability, and legal compliance under the Digital Services Act (DSA), particularly as they relate to the protection of minors online. A central theme across documents is the need for Digital Services Coordinators (DSCs) to have clear, clarified, and non-overlapping mandates, supported by sufficient resources and authority. Many submissions call for harmonized enforcement procedures across the EU, avoiding fragmentation and ensuring coherent implementation. Implementation success is seen as dependent on collaboration among national authorities, the European Commission, and competent bodies, with some highlighting the importance of explicit references to each entity's responsibilities in official guidelines. Cross-platform and supranational coordination mechanisms, such as dedicated reporting systems and shared points of contact, are recommended to enhance responsiveness and prevent regulatory gaps. Some stakeholders also advocate for recognizing new governance models, such as decentralized community-led systems in blockchain environments, and stress the importance of aligning organizational structures—allocating responsibilities not just to compliance teams but across product, growth, and operations. Finally, there is notable debate over whether designating dedicated staff or roles is beneficial or potentially undermines a more integrated approach to accountability.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union. (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown))

Finally, DSCs' role in defending the DSA acquis and these Guidelines in particular is key to prevent a fragmentation of the Single Market. (DOT Europe response1 (DOT Europe))

This person or team should have sufficient resources as well as sufficient authority to have direct access to the senior management body of the provider of the online platform and should also be a central point of contact for regulators and users in matters related to minors' privacy, safety and security. (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 (European Commission))

Die Verbraucherschutzministerinnen, -minister und -senatorinnen der Länder bitten den Bund, dafür Sorge zu tragen, dass die Bundesnetzagentur als deutscher Digital Services Koordinator (DSC) und zuständige Marktüberwachungsbehörde ausreichend ausgestattet wird, um die bestehenden Regelungen des DSA durchsetzen zu können. (TOP 21 Verbot von Tracking, Verhaltensanalysen und Profilbildung zu Werbezwecken (personalisierter Werbung) (Verbraucherschutzministerkonferenz))

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union. (Joint Statement on Article 28 Guidelines (5Rights Foundation))

National consumer protection authorities are responsible for the enforcement of the legislation covering the relevant commercial practices. (Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency))

Contribution Guidelines art 28 DSA (Respect Zone). Highlights the need for coordinated, cross-platform enforcement with standardized procedures for identifying and suspending non-compliant accounts.

Public consultation on 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 (Coimisiún na Meán). Calls for clearer definition of the enforcement and compliance roles of Digital Services Coordinators and inclusion of all competent authorities, beyond just the European Commission, in the guidelines.

the introduction to the guidelines could usefully reflect the use that all competent authorities, in addition to the Commission, will make in supervising and enforcing Article 28.

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Proposes an EU-wide system for reporting and escalating enforcement against persistent bad actors, emphasizing coordination among DSCs, and the need for technical measures such as DNS blocking.

DSCs must coordinate effective enforcement measures, such as DNS blocking and delisting from major search engines.

TOP 21 Verbot von Tracking, Verhaltensanalysen und Profilbildung zu Werbezwecken (personalisierter Werbung) (Verbraucherschutzministerkonferenz). Stresses the importance of adequately resourcing the Bundesnetzagentur as Germany's DSC to ensure robust enforcement of the DSA.

Die Verbraucherschutzministerinnen, -minister und -senatorinnen der Länder bitten den Bund, dafür Sorge zu tragen, dass die Bundesnetzagentur als deutscher Digital Services Koordinator (DSC) und zuständige Marktüberwachungsbehörde ausreichend ausgestattet wird, um die bestehenden Regelungen des DSA durchsetzen zu können.

Adan's response EDPB Guidelines on the processing of personal data through blockchain technologies (Adan). Recommends the recognition of decentralized, community-led governance models in blockchain environments as legitimate within the DSA's scope of accountability and compliance.

The network models assumed by the Guidelines seem outdated, presenting scenarios where a single, unified blockchain network handles the entire data processing operations.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Emphasizes clarifying the DSC's role in implementing and enforcing Article 28(1) for better coherence across the EU.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Requests clarification and alignment of the responsibilities for dedicated personnel under the DSA, and warns against duplication of compliance roles within VLOPs.

As set out above, we feel the proposed new role of the dedicated person duplicates and is inconsistent with the role of the existing Head of Compliance and the compliance function generally pursuant to Art. 41 and we therefore consider it unnecessary.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Advocates explicit guidance on the roles of DSCs, national authorities, and the EC in protecting minors online, and supports coordinated supra-national response mechanisms.

For this reason, AGCOM considers it necessary to include in the Guidelines addressed to online platforms a reference to the role played by DSCs, national authorities, and the European Commission for the application of the DSA obligations on the protection of minors by online platforms and VLOP/VLOSE.

DOT Europe response1 (DOT Europe). Argues for a strong, clarified role for DSCs and the EC to guard against regulatory fragmentation in the protection of minors online.

Finally, DSCs' role in defending the DSA acquis and these Guidelines in particular is key to prevent a fragmentation of the Single Market.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Suggests that compliance responsibilities be communicated across various company divisions, not only a single compliance team, to ensure implementation throughout the organization.

e encourage these guidelines to consider organizational structure, and make it clear that there are expectations for a wide range of company teams, including product and growth teams, to be aware of the regulation and compliance requirements, and to demonstrate changes in how they design, operate, and govern the platform, rather than a single compliance team.

Comments on 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 (Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ)). Supports establishing unambiguous governance roles and providing sufficient resources, emphasizing the critical role of provider competence for DSA compliance.

The Federal Office highly welcomes the emphasis on establishing clear responsibilities accompanied by sufficient resources and authority.

Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act Allwyn submission (Allwyn). Supports cross-border cooperation with national authorities and the use of web-monitoring for enforcement against illegal online content.

We also recognise the role of web-monitoring as an important tool to detect illegal content and expose it to the relevant national authorities.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Calls for clarification of the DSCs' role under Article 28(1) to aid consistent enforcement across EU member states.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union.

EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform). Highlights the necessity of ensuring implementation of current rules and adequate resourcing of new EU mechanisms for combating CSAM.

Ensuring the implementation of the CSAM current rules and the resources of the new EU Center

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Requests clearer definition of DSCs' responsibilities under Article 28(1) for the proper enforcement of minors' protections.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Stresses clarifying the DSC's role in implementation and enforcement under Article 28(1) for coherence across the EU.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Seeks clearer DSC roles with explicit functions, adequate resources, and specialist expertise, along with effective stakeholder engagement for the protection of minors.

elines should require Digital Services Coordinators to: · dedicate specific functions, roles and responsibilities to the protection of minors; · provide them with adequate expertise and resources for the task; · ensure they effectively liaise with counterparts; . ensure that they are an effective and inclusive contact point for children, other citizens or civil society organisations to engage with the authority on the protection of minors, as well as for companies to be advised on compliance.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Expresses willingness to collaborate with the EC to fulfil DSA requirements and improve child safety online.

We look forward to working with the EC as we continue our efforts to address this important issue.

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 (European Commission). Recommends assigning dedicated, well-resourced specialists or teams with authority over minors' privacy and security, serving as central points of contact.

This person or team should have sufficient resources as well as sufficient authority to have direct access to the senior management body of the provider of the online platform and should also be a central point of contact for regulators and users in matters related to minors' privacy, safety and security.

Joint Statement on Article 28 Guidelines (5Rights Foundation). Supports further clarification of the DSCs' role for coherent DSA enforcement regarding minors.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Argues against mandating dedicated staff for minors' safety, suggesting such requirements may inhibit effective internal resource allocation and integrated accountability.

The requirement to have a 'dedicated' team or person risks undermining the shared nature of this responsibility and the ability of providers to manage internal resources appropriately and effectively (both from a user safety perspective and operationally).

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Reiterates the call for more explicit guidance on DSCs' responsibilities to assure EU-wide coherence in enforcement.

The role of Digital Services Coordinators in regard to article 28(1) should further be clarified, especially regarding their uptake of the guidelines, to ensure coordinated and coherent implementation and enforcement across the Union.

Feedback on the draft Commission guidelines on DSA article 28 (Swedish Agency for the Media). Requests greater clarification on how DSA enforcement overlaps or interacts with consumer protection authorities at the national level.

It is not entirely clear how supervision carried out by national authorities competent for DSA article 28 relates to supervision carried out by national consumer protection authorities (with regard to consumer protection legislation).

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Suggests more specificity in defining the uptake and enforcement roles of DSCs under Article 28(1).

We suggest to better clarify the role of Digital Services Coordinators on their uptake of the guidelines.

Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency). Warns against overlap in enforcement mandates between DSA and national consumer protection authorities, advocating for clear boundaries in the guidance.

There's a risk for overlap if these practices, through the inclusion in the guidance, are considered to fall under Article 28(1), and thereby is subject to enforcement of DSA authorities.

1.13.3 Guidance, Proportionality, and Support

The insights in "Guidance, Proportionality, and Support" stress the importance of clear, actionable guidance for stakeholders implementing the Digital Services Act (DSA), particularly concerning the protection of minors online. Contributors repeatedly emphasize the need for regulatory clarity—through concise definitions, practical examples, and transitional periods—to ensure legal certainty and effective compliance. There is strong consensus on proportionate enforcement, recommending that guidelines align with the capacities of organizations, especially SMEs and micro-enterprises, to prevent undue burdens and maintain a competitive digital landscape. The insights further recognize the value of supportive, non-binding guidelines designed to inspire best practices, rather than to create additional de facto obligations beyond the DSA. Calls are also made for flexible approaches, integration of all types of providers, and proactive support (e.g., public funding, templates for risk assessment, industry codes). Several responses highlight the need for harmonized and binding references where fragmentation would hinder effectiveness, but most insist any benchmarks should remain pragmatic, non-duplicative, and allow for adaptation to sectoral differences. The overall tone promotes balanced, practical, and staged implementation, with special attention to the needs of minors and vulnerable users.

As the digital regulatory landscape continues to evolve, clear and concise regulatory guidance is a key tool to assist organisations in understanding regulatory expectations and create legal certainty. (Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)))

ZPP stresses that the implementation of these guidelines must be proportionate and mindful of the limited resources of small and medium-sized enterprises (SMEs). (Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)))

It should be reiterated that these are not binding rules but supportive guidance by best practises to assist in the implementation and enforcement of existing obligations. (Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry))

However, for the guidelines to be truly effective, all online service providers, including providers of online platforms that qualify as micro or small enterprises, should use these guidelines as a source of inspiration, despite the exemption in Article 19 of the DSA. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

In addition, key concepts require stable and operational legal definitions, notably: "age-appropriate design," "harmful content," and "at-risk interaction." (Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018))

We recommend that additional guidance be introduced to clarify the Commission's position on this point. (TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited))

Response by the Centre for Information Policy Leadership to the European Commission's Draft Guidelines under Article 28 of the DSA (Centre for Information Policy Leadership (CIPL)). This document highlights the necessity of clear and concise regulatory guidance, as well as advocating for a transitional implementation period to aid organizations in adapting to the DSA.

Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)). The submission stresses the importance of proportionality in compliance, tailored SME support, and the inclusion of safe-harbour provisions to protect compliant platforms.

ZPP stresses that the implementation of these guidelines must be proportionate and mindful of the limited resources of small and medium-sized enterprises (SMEs).

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). It calls for public funding and strategic procurement policies to support digital rights initiatives and ensure technologies align with ethical and civic goals.

Public funding, such as the European Commission's Next Generation Internet (NGI) of Trust, align technology with ethical guides on Public Digital Infrastructure and the UN's Global Digital Act that advance digital rights, public participation, and social trust.

UCD_Centre_for_Digital_Policy_Art_28 (UCD Centre for Digital Policy). Advocates setting more rigid language and establishing baseline safety, accessibility, and recourse standards for platforms, with practical tools to support under-resourced regulators.

We recommend that the language of the Guidelines becomes more rigid, and baseline requirements are set for platforms proposing specific design requirements for safety, accessibility and recourse.

Comments on the European Commission draft 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 ("DSA") (BDZV, MVFP). This response argues editorial platforms should be exempt from extra DSA obligations due to their existing high standards and the disproportionate burden further requirements would impose.

By implementing the DSA obligations and already fulfilling the present guidelines' core objective of ensuring a high level of privacy, safety and security, editorial online platforms should be explicitly excluded from requirements to implement additional measures prescribed in the guidelines.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). The document asks to clarify that for Very Large Online Search Engines (VLOSEs), DSA guidelines should be considered inspirational rather than directly binding, due to their fundamental differences.

It should be clarified that for Very Large Online Search Engines (VLOSEs), the guidelines may be inspirational, but not directly relevant both due to the scope of Article 28 DSA and the fundamentally different nature of search engine services.

Additional contribution (Collective Shout). It supports consolidated industry codes of practice as a framework for complying with child protection measures online.

Submission to Consolidated Industry Codes of Practice for the Online Industry.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Emphasizes the need for further development and clarification of the guidelines to fully uphold children's rights under Article 28.

Although, according to Bris there are areas within the guidelines that requires further development and clarification to uphold the protection of children's rights under Article 28 of the DSA.

DOT Europe response1 (DOT Europe). Recommends more detailed clarification of terminology and practical risk indicators in the guidelines to aid platforms in compliance with the DSA.

the final Guidelines should clarify some concepts further in order to help online platforms be compliant with it, for example: "high risk" and "medium risk" services (including indicators of what constitutes the respective risk level), the proportionality of chosen measures, "significant change" requiring the conduct of another risk review and when an online platform is deemed to be out of scope (how many minor users is "some"?).

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). Warns against creating excessive or unfair burdens on platforms, emphasizing legal coherence, competitiveness, and privacy-preserving, risk-based measures.

In any case, it seems essential to ensure that these measures do not become a barrier to the competitiveness of European businesses, insofar as (i) they create friction in the user experience and (ii) represent a particularly significant cost for smaller organisations.

Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (INHOPE). Identifies a structural weakness in excluding micro and small businesses from guideline requirements, and suggests integrating them within a minimal liability framework for child protection.

We understand the logic of proportionality with regard to these small players and the desire for consistency with the graduated system arising from the DSA architecture, but in the interests of child protection, we call for additional measures to integrate these at-risk players into a minimum liability regime.

Feedback on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Association e-Enfance/3018). Calls for the guidelines to be formalized and harmonized as binding standards to unify protection measures for minors across the EU.

In a context of fragmented regulatory responses, it is imperative that this text be established as a binding and harmonised reference, fully implemented across all Member States.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Proposes a flexible 'duty of care' obligation for publishers, prioritizing minors' interests over corporate ones and extending certain protections to all users.

Instead of enumerating specific restrictions, lawmakers can require publishers to satisfy a duty of care to treat minors "better" than adults, prioritize the best interests of minors, or otherwise subvert their corporate interests in favor of minors' interest

Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance). Promotes enforcement approaches that are proportional to platform risk, non-duplicative, and pragmatic to avoid unnecessary burdens.

Default settings should be proportionate to the platform's actual risk profile and the nature of its services.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Urges that all online service providers, including micro and small enterprises, use the guidelines as inspiration and refrain from launching services if standards cannot be met.

If online platforms cannot meet these standards, they should not be allowed to launch their services and products.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Arcom recommends maintaining high ambition in the final guidelines and ensuring their rapid and effective implementation.

De plus, l'Arcom appelle la Commission à adopter rapidement les lignes directrices et à veiller avec diligence à ce qu'elles soient appliquées promptement après leur publication, avec des résultats rapides et tangibles sur les plateformes pour les citoyens européens.

Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA) (eco Association of the Internet Industry). Insists that guidelines remain non-binding and flexible, serving as supportive best practice without introducing new obligations beyond those legislated under the DSA.

It should be reiterated that these are not binding rules but supportive guidance by best practises to assist in the implementation and enforcement of existing obligations.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Requests further clarity regarding the additional compliance expectations for Very Large Online Platforms, reaffirming the guidelines as a benchmark for assessment.

We welcome confirmation from the Commission that the Guidelines equally represent a "significant and meaningful benchmark on which the Commission will base itself" when assessing compliance of providers of VLOPs with Section 5 of Chapter III DSA.

Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act (Electronic Frontier Foundation). Calls for differentiation of obligations between smaller providers and VLOPs, as well as additional guidance to prevent disproportionate burdens on smaller platforms.

Providers of smaller online providers are often less versed in the assessment of complex risks than very large online platforms (VLOPs) and search engines (VLOSEs) and usually have significantly fewer resources available.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Asks for clarification of subjective terms like 'state-of-the-art' and how compliance with DSA obligations relates to benchmark requirements in the guidelines.

The term "state-of-the-art" sets a benchmark which is subjective and difficult to demonstrate compliance against.

On the concept of personal integrity in the german protection of minors (unknown). Suggests exempting platforms with fewer than one million users from certain precautionary DSA measures, aligning with existing labeling rules.

In analogy to the labelling requirement pursuant to § 14a, platforms with fewer than one million users in Germany are also exempt from taking precautionary measures in this case.

DSA Guidelines for Protection of Minors Additional Submission EuroISPA FINAL (EuroISPA). Emphasizes maintaining the non-binding status of guidelines and avoiding overlapping or excessive obligations, particularly in relation to VLOPs.

It must be clearly mentioned that guidelines are non-binding and should not introduce new legal obligations excluded during the DSA legislative process.

Consultation Response from Barnevakten, Norway - Regarding Article 28 of the EU Commission's Digital Services Act (DSA) (Barnevakten Foundation). Accepts the current exemption threshold for small companies as reasonable, cautioning against overly onerous requirements for small businesses in the absence of further experience.

However, the current threshold seems acceptable until there is more experience with how the rules work in practice.

1.13.4 Accountability, Oversight, and Redress

This category emphasizes the urgent need for clear, robust mechanisms of accountability, oversight, and redress in the enforcement of guidelines under the EU Digital Services Act (DSA), particularly regarding the protection of minors. Insights are diverse, spanning proposals for strong regulatory oversight (with dedicated roles for Digital Services Coordinators and national authorities), requirements for clear timelines and regular stakeholder consultation, integration of self- and co-regulatory approaches, and structures for both internal and external complaint and redress systems. There is strong advocacy for creating real personal (civil and criminal) liability for public or platform decision-makers in cases of gross negligence and calls for enabling children and their guardians to seek remedies in courts. Several contributions stress the importance of continuous monitoring, institutional safeguards, independent audits, and systems modeled on successful certification or compliance programs from other sectors (e.g., LEED, B Corp, ESG). Others highlight the critical absence or insufficiency of redress mechanisms, whistleblowing, and internal escalation options, leaving minors vulnerable to platform decisions without oversight or appeal. Overall, there is consensus that accountability and oversight must not be merely formal duties but translated into transparent, operational, and enforceable actions, ensuring the safety and rights of minors online.

> *A review threshold is crucial to hold regulators, especially the Digital Service Coordinators, on implementing these guidelines and ensure that these provisions effectively contribute to the goal of Article 28(1).* (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))
>
> *Individual children and parents should be able to hold online platforms to account in courts for harm done.* (CONCLUSION & POLICY DEMANDS (unknown))
>
> *Article 20 of Regulation (EU) 2022/2065 requires providers of online platforms to provide recipients of the service with access to an effective internal complaint-handling system against four types of decisions taken by the provider of the online platform.* (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 (European Commission))
>
> *Individual children and parents should be able to hold online platforms to account in courts for harm done.* (CONCLUSION & POLICY DEMANDS (unknown))
>
> *Effective and already established international and national self-regulatory protection mechanisms and procedures for the protection of minors on online platforms are therefore not sufficiently taken into account.* (Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)))
>
> *de actieve bescherming van kinderen vanuit de technologiebedrijven, in plaats van te rekenen op vrijwillige gedragscodes.* (Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Stresses the importance of a strong review threshold, effective oversight, and clarity of roles for Digital Services Coordinators to ensure robust implementation of minors' protection guidelines.

CONCLUSION & POLICY DEMANDS (unknown). Argues that children and their parents should have the ability to pursue legal accountability against platforms causing harm under the DSA.

Individual children and parents should be able to hold online platforms to account in courts for harm done.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Proposes a professional, independent certification system for prosocial technology design, administered by a nonprofit and modeled after established sustainability and ethics standards to enhance accountability.

A Professional Certification System for Prosocial Technology Tiers could recognize platforms, products, and practitioners achieving distinct tiers of prosocial technology design.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU)

2022/2065 (Bris). Calls for both the European Commission and national authorities to take full, active supervisory roles to ensure effective and consistent compliance with guidelines across the EU.

It also requires the European Commission and national authorities to fully assume their supervisory responsibilities, ensuring that compliance with the guidelines is consistent and effective across all platforms.

Statement by the Entertainment Software Self-Regulation Body (USK) (Entertainment Software Self-Regulation Body (USK)). Highlights the untapped value of proven self-regulatory approaches and urges their integration into DSA enforcement for platforms, especially in the context of youth protection.

In the USK's view, there is clearly unused potential in the lack of consideration of proven effective models for preventive, self-regulatory approaches.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Advocates introducing personal civil and criminal liability for public officials in cases of gross negligence and calls for greater transparency and accountability in regulatory processes.

equired Solution: · Personal civil and criminal liability for gross negligence

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Suggests mandating civil and criminal liability for public officials' gross negligence, along with compulsory suspension of digital services not compliant with minors' safety requirements.

quired Solution: · Personal civil and criminal liability for gross negligence

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Emphasizes the need for whistleblowing, internal escalation mechanisms, and redress opportunities to protect children from decisions by platforms made without effective oversight.

This lack of redress mechanisms leaves children vulnerable to platform decisions made without meaningful oversight or appeal processes.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Calls for direct individual accountability measures for forcing minors to use unsafe digital platforms.

Individual accountability for forcing minors to use unsafe platforms

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 (European Commission). Details the DSA-mandated requirement for platforms to establish effective internal complaint-handling systems for users affected by several types of decisions.

Article 20 of Regulation (EU) 2022/2065 requires providers of online platforms to provide recipients of the service with access to an effective internal complaint-handling system against four types of decisions taken by the provider of the online platform.

Greece’s contribution to the open consultation on the European Commission’s draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Recommends setting timelines for accountability, regularly updating guidelines in consultation with relevant stakeholders, and strengthening institutional safeguards for minors.

We recommend setting clear timelines for accountability purposes.

Nota voor Commissie Cultuur, Jeugd, Sport en Media (KidsUnplugged). Insists on the active duty of care and legal liability of technology companies for the consequences of their platforms on children, rather than relying on voluntary codes.

Het is van cruciaal belang dat die bedrijven de zorgplicht hebben voor de gevolgen van hun producten en diensten, en dat ze aansprakelijk worden gesteld indien ze geen duidelijke en implementeerbare acties ondernemen;

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Asserts that current guidelines insufficiently address redress and contingency support for minors, and references interoperability and technical certification standards as supportive mechanisms.

Yes, the draft guidelines do not contain sufficient coverage for redress and contingency support for minors, particularly among services most frequently used by children and adolescents.

Consultation Response from Barnevakten, Norway - Regarding Article 28 of the EU Commission's Digital Services Act (DSA) (Barnevakten Foundation). Notes the possibility of platforms offering differentiated services across countries, thus requiring close and ongoing national authority oversight for local compliance.

It is also possible that platforms will offer differentiated services in different countries, meaning that national authorities will need to closely monitor whether platforms comply with the rules locally.

1.13.5 Procedural Clarity and Review

The documents grouped under 'Enforcement, Accountability, and Legal Compliance >> Procedural Clarity and Review' underscore the importance of clear, consistent, and enforceable procedures for the implementation and ongoing governance of the Digital Services Act's (DSA) protections for minors. Key themes include the necessity of regular and responsive review processes for guidelines—often recommending specific timelines such as a two-year or five-year review period, with flexibility for earlier updates based on technological or regulatory changes. There is a strong emphasis on establishing clear standards for enforcement readiness prior to implementing measures like age verification, and on ensuring that compliance assessments consider both the effectiveness and practical adoption of measures, rather than just formal implementation. Procedural clarity extends to the definition of key terms (such as what constitutes a 'platform accessible to minors'), the need for transparent and harmonized requirements (such as for complaint categories, audit data retention, and financial independence of trusted flaggers), and the provision of grace periods for platforms to adapt to new guidelines. Several insights highlight the risk of legal uncertainty, advocating for greater legal certainty and predictable 'safe harbor' for platforms that fully comply. There are also calls to strengthen accountability by shifting language from permissive ('should') to mandatory ('must'), and suggestions for fast-track enforcement protocols, defined escalation procedures, third-party audits, and outcome-based compliance assessments. Overall, the documents advocate for a balance between robust procedural safeguards, practical enforceability, and flexibility to adapt guidelines in response to evolving challenges. Platforms, regulators, and oversight bodies are urged to coordinate actions transparently, ensuring measures are both clear and effective in practice.

The Commission will review these guidelines two years after their adoption, or as soon as this is necessary in view of practical experience gained in the application of that provision and the pace of technological, societal, and regulatory developments in this area (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

As to the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments. (SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands))

Notwithstanding the above, the Guidelines state: "Nevertheless, adopting and implementing measures set out in these guidelines, either partially or in full, shall not automatically entail compliance with that provision.". (Feedback for 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 (xHamster))

Typically, when platforms adhere to all recommended guidelines, they are afforded a form of 'safe harbor' in regards to their compliance. (Feedback for 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 (xHamster))

It should also be defined more clearly what are the consequences if not enough effort is put into the risk review. (STATEMENT (Digipeace (Digirauha ry)))

In this regard, AGCOM considers it appropriate to consider the Guidelines as a benchmark for authorities and the Commission and suggests qualifying them as a parameter for the exercise of supervisory discretion rather than as a "limit" to the exercise of such discretion (lines 115 and 116). (AGCOM's observations on the European Commission's public consultation on the Guidelines on

measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)))

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). This document highlights the need for clear enforcement thresholds and user acceptance criteria before rolling out mandatory age verification, warning that premature implementation could lead to significant user migration to less-regulated platforms.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). The submission emphasizes the importance of regular review of the guidelines—proposing an initial two-year period—and flexibility for earlier updates based on technological, societal, or regulatory developments.

The Commission will review these guidelines two years after their adoption, or as soon as this is necessary in view of practical experience gained in the application of that provision and the pace of technological, societal, and regulatory developments in this area

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). AFNUM stresses the necessity of a precise definition for platforms accessible to minors to enable consistent and practical enforcement of protective measures.

nous considérons qu'une définition précise de la notion de « plateforme accessible aux mineurs » est indispensable pour garantir la mise en œuvre pratique des mesures.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). AGCOM advises that the DSA Guidelines should serve as benchmarks guiding the supervisory discretion of authorities and the Commission, not as restrictive limits.

In this regard, AGCOM considers it appropriate to consider the Guidelines as a benchmark for authorities and the Commission and suggests qualifying them as a parameter for the exercise of supervisory discretion rather than as a "limit" to the exercise of such discretion (lines 115 and 116).

Yoti_response_on_Article_28__2_.pdf (Yoti). Yoti requests clarity regarding audit data retention policies—such as duration, encryption, and requirements for third parties—in the event of investigations under the DSA.

provide clarity as to what are the requirements on age assurance providers, after an age check, to retain audit data, what, how long, encrypted etc ...

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). This document calls for robust compliance verification processes, including specific medium-term timelines and fast-track enforcement procedures with clear deadlines.

Fast-track enforcement procedures (maximum 90 days)

SUBMISSION BY DEFENCE FOR CHILDREN - NETHERLANDS ON DRAFT GUIDELINES UNDER ARTICLE 28(1) OF THE DIGITAL SERVICES ACT (Defence for Children - ECPAT the Netherlands). Defence for Children - ECPAT emphasizes establishing a two-year review period for children's guidelines, as well as clarifying the role of Digital Services Coordinators to ensure harmonized implementation across the EU.

As to the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

STATEMENT (Digipeace (Digirauha ry)). Digipeace calls for stronger escalation procedures and clearer consequence definitions when platforms fail to adequately protect children or address risks.

It should also be defined more clearly what are the consequences if not enough effort is put into the risk review.

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Homo Digitalis urges the replacement of non-binding language ('should') with binding requirements ('must') to ensure stronger enforceability for child rights impact assessments.

The repeated use of "should" instead of "must" throughout the document significantly weakens the enforceability of these critical protections, creating a permissive rather than mandatory framework that may allow platforms to treat child safety measures as optional recommendations rather than binding obligations.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). COFACE Families Europe recommends that enforcement of Article 28(1) focus on actual outcomes for child protection, not merely the adoption of formal measures.

Nevertheless, it is important that compliance to Article 28(1) is not merely judged based on the measures per se adopted by providers of online platforms but on the outcomes of those measures.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Thorn advocates for a mandatory review timeline of 24 months for the guidelines, with additional flexibility to allow earlier updates as needed.

Set a mandatory review timeline of 24 months, with flexibility for faster reviews in response to regulatory or technological changes

The Danish government's response to the Commissions consultation regarding Article 28 of the Digital Services Act (The Danish Government). The Danish Government supports the regular review of the guidelines, suggesting at least a five-year maximum interval, but with provisions for earlier updates in response to relevant developments.

The Commission will review these guidelines as soon as this is neces- sary in view of practical experience gained in the application of that provision and the pace of technolog- ical, societal, and regulatory devel- opments in this area, and in no later than 5 years.

Feedback for 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 (xHamster). xHamster identifies inconsistencies between requirements in the guidelines and underlying regulation, calling for clarification, harmonization, and legal certainty—especially regarding 'safe harbor' for compliant platforms.

Greater legal certainty is therefore essential.

EASA contribution to the European Commission's draft DSA Guidance on the Protection of minors (European Advertising Standards Alliance). EASA seeks clarification on the financial independence requirements for organizations acting as 'trusted flaggers' or providing out-of-court dispute resolution under the DSA, ensuring these requirements are fair and practical.

The financial independence requirements under DSA Article 21 and 22 should be clarified.

Joint Statement on Article 28 Guidelines (5Rights Foundation). 5Rights Foundation advocates for a regular two-year review period for the guidelines, with an option for expedited updates if needed.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). TikTok calls for a minimum six-month grace period for compliance implementation before formal assessments take place under the DSA guidelines, recognizing the practical effort required.

TikTok recommends that the Commission takes this into account when finalising the Guidelines and provides a period of at least six months for services to make any changes required before any formal compliance assessments take place.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This statement recommends establishing a two-year guideline review cycle, with allowances for earlier revisions prompted by new regulatory or technological developments.

As for the guidelines, a clear review period of 2 years should also be established, while allowing for earlier review if required by technological, societal or regulatory developments.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Technology Ireland proposes granting platforms a minimum twelve-month grace period to assess and adapt to applicable guidelines before enforcement, emphasizing the need for proportionate and effective implementation.

Platforms should be granted a reasonable grace period, at least twelve months, to assess which "Guidelines" apply to them and to implement a tailored compliance programme.

1.13.6 Enforcement Mechanisms and Sanctions

The category 'Enforcement Mechanisms and Sanctions' encompasses widespread calls for the implementation of robust and mandatory enforcement measures to ensure that online platforms adhere to digital safety rules protecting minors. Key recommendations across documents emphasize that compliance with regulations, particularly the EU Digital Services Act (DSA), must not be voluntary. Typical enforcement proposals include a mix of fines, operational restrictions or shutdowns, and legal liability for non-compliance, aiming to deter infractions through real and tangible consequences. Several documents highlight the need for harmonized, cross-jurisdictional enforcement, auditable accountability practices, and the application of consistent standards across different platforms. There is advocacy for innovative sanctions such as digital banishment against repeat offenders and the codification of product liability to address systemic social harms. A growing consensus emerges around the inadequacy of voluntary or self-regulated compliance models, thus underscoring the necessity for mandatory and well-defined enforcement mechanisms backed by regulatory authorities. Additionally, the insights reflect a push for periodic audits, effective oversight, and transparent processes to identify, investigate, and penalize non-compliance while advocating for child-centered, proactive enforcement strategies that consider both technical and societal dimensions of platform accountability.

Set up enforcement mechanisms (e.g. fines, shutdowns, legal liability), so that compliance is not left on a voluntary basis for platforms. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

Set up enforcement mechanisms (e.g. fines, shutdowns, legal liability), so that compliance is not left on a voluntary basis for platforms. (Ten recommendations to the European Commission to really protect children online (unknown))

Without enforceable mechanisms such as fines, legal liability, or operational restrictions, compliance with the guidelines remains voluntary. (Policy_demands (unknown))

Individual children and parents should be able to hold online platforms to account in courts for harm done. (Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union))

C2. Codify Product Liability for Adverse Impacts (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Fast-track enforcement procedures (maximum 90 days) (Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown))

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Proposes establishing enforcement mechanisms such as fines, shutdowns, and legal liability to make compliance with online child protection rules mandatory for platforms.

Contribution Guidelines art 28 DSA (Respect Zone). Suggests generalizing the use of digital banishment as a complementary judicial sanction, particularly for offences like cyberbullying or hate speech, to prevent recidivism and promote accountability.

Generalizing the use of digital banishment as a complementary sanction, in cases of cyberbullying, non-consensual image sharing, or hate speech (in line with Article 16 of the French SREN law);

Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.). Stresses the need for uniform enforcement of age-assurance obligations and harmonized standards across Member States to avoid conflicting regulations for platforms.

Where providers comply with these guidelines, Member States should not impose additional or conflicting age-assurance obligations.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Calls for the set up of mandatory enforcement mechanisms and deterrents such as fines and shutdowns, highlighting that clear rules alone are insufficient without credible sanctions.

Set up enforcement mechanisms (e.g. fines, shutdowns, legal liability), so that compliance is not left on a voluntary basis for platforms.

Consultation Submission Summary: Strengthening Platform Accountability to Protect Minors from Pornographic and Age-Inappropriate Content under DSA Guidelines (Asociación Stop Porn Start Sex España). Advocates for effective enforcement measures and significant penalties to address both non-compliance and platform designs that intentionally circumvent regulations.

Effective enforcement measures and meaningful penalties for non-compliance or platform designs that enable circumvention.

Ten recommendations to the European Commission to really protect children online (unknown). Reiterates the need for enforcement mechanisms (fines, shutdowns, legal liability) and credible deterrents to ensure compliance and effective regulation.

Set up enforcement mechanisms (e.g. fines, shutdowns, legal liability), so that compliance is not left on a voluntary basis for platforms.

Stellungnahme zur öffentlichen EU Konsultation: Leitlinien der Kommission für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre und Sicherheit für Minderjährige im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022 / 2065 (Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg). Emphasizes the importance of consistent application of sanctions as part of enforcement for improving online safety for minors.

Sanktionierungen konsequent einzusetzen

SUBMISSION TO THE PUBLIC CONSULTATION ON THE DSA GUIDELINES ON THE PROTECTION OF MINORS (Amnesty International). Supports the enforcement of due diligence and responsible business conduct standards for online platforms in alignment with the DSA.

OECD Due Diligence Guidance for Responsible Business Conduct, 2018,

CONCLUSION & POLICY DEMANDS (unknown). Highlights the need for proportionate, enforceable obligations and the establishment of mechanisms like fines and shutdowns for compliance with child safety rules.

Safety must be embedded across the entire digital value chain — not delegated solely to front-facing platforms.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Proposes the codification of product liability to make tech companies accountable for systemic societal risks, moving beyond traditional financial metrics.

Codifying product liability holds tech companies accountable for systemic risks like polarization, privacy violations, and disinformation.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Calls for codified product liability for

platform design harms and regulation of deceptive design patterns as means to reduce digital risks for minors.

Codifying product liability for the adverse social impacts of platform design is essential to reducing digital harm because it shifts accountability from individual users and content moderation to the systemic design choices that drive large-scale societal risk.

Ten recommendations to the European Commission to really protect children online (unknown). Underlines that enforceable mechanisms such as fines, shutdowns, and legal liability are needed to prevent voluntary compliance and ensure regulation has deterrent effect.

Set up enforcement mechanisms (e.g. fines, shutdowns, legal liability), so that compliance is not left on a voluntary basis for platforms.

Safe by Default (Panoptykon Foundation). Recommends strong enforcement of DSA provisions specifically aimed at the vulnerabilities and rights of children regarding algorithmic recommender systems.

E]nsure strong enforcement of the Digital Services Act on the matter, with a focus on provisions on children and special consideration of their specific rights and vulnerabilities.

AGCOM's observations on the European Commission's public consultation on the Guidelines on measures to ensure the protection of minors online pursuant to Article 28(4) of the Digital Services Act - Regulation (EU) 2022/2065 (AGCOM (Italian Communications Authority)). Supports the recall and application of sanctioning measures in cases of Article 28 DSA violations, emphasizing clarification and interpretative guidance for enforcement.

AGCOM considers it useful to recall the sanctioning measures in cases where Article 28 of the DSA is violated, for which the Guidelines provide interpretative criteria for compliance.

Policy_demands (unknown). Advocates for establishing enforcement mechanisms with sanctions since, without them, guidelines risk remaining voluntary and unenforceable.

Without enforceable mechanisms such as fines, legal liability, or operational restrictions, compliance with the guidelines remains voluntary.

II Input on the Protection of Minors Guidelines under the Digital Services Act (Integrity Institute). Argues that enforcement should focus on the majority of responsible child users and acknowledges that complete circumvention is unavoidable by motivated minors.

It is critical for the Commission to focus on the majority of child users who intend to use platforms responsibly, rather than the minority who attempt to skirt regulation.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Recommends real enforcement mechanisms, technical audits, and even mandatory suspension of non-compliant services for data protection violations.

Only mandatory standards with real consequences will protect minors online.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Stresses the need for prompt initial enforcement actions and the implementation of effective mechanisms after guidelines adoption.

First enforcement actions

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Focuses on the implementation of enforcement mechanisms and the necessity of first enforcement actions to establish compliance controls.

Enforcement mechanism implementation

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Emphasizes enforcing existing online safety laws by ensuring sufficient law enforcement capacity to address online threats against children.

Enforce Existing Laws. Children face a wide range of threats online, but existing laws already regulates many of those threats. We should ensure that we have enough law enforcement officers "walking the virtual beat" to proactively thwart (and deter) those threats and to appropriately prosecute violations.209

Art. 28 DSA Leitlinien Stellungnahme der Medienanstalten (Medienanstalten). Identifies a lack of provider readiness to implement age verification systems as a barrier, calling for increased enforcement to ensure protection of minors.

bschließend möchten die Medienanstalten betonen, dass ihre Erfahrungen der Medienanstalten in der Durchsetzung zeigen, dass es nicht an ausreichenden Systemen der Altersprüfung bzw. Altersschätzung mangelt, sondern überwiegend an der Bereit- schaft der Anbieter, diese Systeme zum Schutz von Minderjähri gen zu implementieren.

Securing a high level of privacy, safety and security for minors online (SUPERRR Lab). Suggests shifting regulatory focus to user well-being and enforcement—away from platform-centered, self-regulatory technical tools and towards addressing exploitative design.

Rather than offering technical tools that enable platforms to maintain extractive business models, the focus should be on regulatory enforcement, promoting alternatives that center user well-being, and addressing the root causes of exploitative design and commercial practices.

STATEMENT (Digipeace (Digirauha ry)). Recommends stronger enforcement provisions and independent auditing standards, as well as sanctions reflecting the seriousness of harm to minors.

The Guidelines should have stronger provisions for:

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Argues that the effectiveness of the DSA depends on enforcement and calls for auditable platform accountability in applying settings for minors.

There should be auditable accountability on how platforms apply and enforce default settings for minors.

Feedback DSA (unknown). Calls for increased transparency and practical clarity around how enforcement mechanisms in the guidelines will function.

The document would benefit from clarifying how the proposed guidelines will be enforced in practice.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Recommends that the Commission develop an enforcement priority action plan, giving precedence to very large platforms and those posing the greatest risk to minors.

À cet égard, il est essentiel que la Commission établisse, en lien avec les coordinateurs pour les services numériques (Digital Services Coordinators - DSC ou CSN), notamment dans le cadre du Comité européen des services numériques (DSA Boardou Comité), un plan d'actions détaillant ses priorités vis-à-vis des VLOPSEs (Very Large Online Platforms and Search Engines) en premier lieu, mais également des plateformes en ligne qui présentent le plus de risques pour les mineurs.

Additional Contribution to DSA Article 28(4) Guidelines Public Consultation (unknown). Advocates banning manipulative designs, implementing mandatory enforcement mechanisms, and imposing a moratorium on AI use for minors.

Only mandatory standards with real consequences will protect minors online.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Encourages the European Commission to use its full suite of enforcement powers to guarantee systemic and consistent compliance across platforms.

Equally, it is essential that the European Commission makes full and timely use of its supervisory, investigatory and enforcement powers to ensure that compliance is not optional, but systemic, consistent and effective across platforms.

Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology). Emphasizes enforcement of the DSA guidelines to actually realize children's rights, implementing principles such as safety and privacy by design.

They must also be enforced diligently, proactively and in a manner that truly realises children's rights.

Additional recommendations and comments on the draft guidelines (Mediahealth for children and youth). Urges EU-wide harmonized enforcement of age assurance measures to enhance online child protection.

Encourage EU-wide collaboration for harmonized enforcement.

Feedback for 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 (xHamster). Proposes strengthening age assurance and enforcement, introducing automated reporting of non-compliance, and ensuring a level playing field for platforms.

To address these challenges, a comprehensive enforcement plan is imperative.

Ten recommendations to the European Commission to really protect children online (unknown). Pushes for enforceable compliance mechanisms (fines, shutdowns, legal liability) to keep platforms accountable, highlighting that deterrents are as crucial as the rules themselves.

Set up enforcement mechanisms (e.g. fines, shutdowns, legal liability), so that compliance is not left on a voluntary basis for platforms.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Notes that stronger measures are required from the Commission to strictly enforce and ensure platform accountability for minor safety and privacy.

We welcome the intent of the guidelines to provide clear actionable guidance to online platforms, however we believe the Commission should utilise stronger measures to strictly enforce and hold platforms accountable for ensuring the Privacy, Safety and Security of minors.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Supports making enforcement measures for children's rights mandatory, as voluntary action is insufficient despite providers' capability.

We support the guideline outlined in line 535-538 but recommend that these measures are made mandatory.

Ten key common recommendations to the European Commission TO PROTECT CHILDREN AND TEENAGERS ONLINE (Parents' Apolitical Movements Across the Union). Insists that, without strong enforcement mechanisms such as fines and legal liability, compliance with online safety guidelines for minors will remain voluntary and lacking in real impact.

Without enforceable mechanisms such as fines, legal liability, or operational restrictions, compliance with the guidelines remains voluntary.

1.13.7 Miscellaneous

1.14 Interoperability, Standards, and Ecosystem Responsibilities

The most compelling insight emerging from these sub-categories is the imperative for harmonized, ecosystem-wide collaboration—spanning platforms, device makers, telecoms, and regulators—to ensure that the protection of minors online is cohesive and robust. Rather than confining responsibility to individual companies, "protective obligations are clear and enforceable for all relevant actors," fostering a culture of shared

accountability across the entire digital value chain. Harmonized technical standards, such as CWA 18016/IEEE 2089, are consistently highlighted as foundational for effective child safety, particularly for "cross-platform and cross-device interoperability" of parental controls and risk mitigation tools. This technical alignment is complemented by strong calls for unified legal frameworks and EU-level guidance to prevent regulatory fragmentation, streamline compliance, and clarify overlaps between major regulations like the DSA, GDPR, and AVMSD. Adaptability—modifying technologies for cultural and local specifics—is also essential to ensure inclusivity. Competition and interoperability policies further reinforce this approach, by requiring open APIs, data portability, and prevention of 'walled gardens,' making high standards universally accessible and enforceable, particularly for prosocial and smaller platforms. Across all threads, a consistent trend emerges: safeguarding minors online depends on integrated, legally coherent, and technically interoperable solutions, built through cross-sectoral cooperation and enabled by strong, harmonized guidance and standards.

1.14.1 Ecosystem Collaboration and Responsibility

The category 'Ecosystem Collaboration and Responsibility' encapsulates the growing consensus that effective protection of minors online necessitates a collaborative, ecosystem-wide approach. Key insights stress that responsibility for online safety cannot rest solely with front-facing online platforms; it should be distributed across the entire digital value chain, including device manufacturers, telecom providers, education technology platforms, and service intermediaries. Interoperability and shared responsibilities are emphasized, urging regulatory guidelines to incentivize cross-sector cooperation and ensure that protective obligations are clear and enforceable for all relevant actors. Additionally, many stakeholders advocate for active data sharing, the exchange of best practices, and robust coordination not just between platforms, but also involving government, regulators, industry bodies, and civil society organizations. There is a call for technology-neutral and harmonized standards to avoid uneven regulatory landscapes, as well as mechanisms for coordinated oversight and enforcement—especially across borders—so minors are protected consistently regardless of where or how they access digital services. Finally, several contributors highlight the importance of embedding safety measures and risk mitigation throughout the ecosystem—from default device settings to educational tech safeguards—and recommend periodic review and cooperation on emerging threats. The collaborative approach is seen as fundamental to a safer, more resilient digital environment for children.

> *The guidelines should therefore incentivise interoperable solutions and shared responsibility among all actors.* (Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)))
>
> *Safety must be embedded across the entire digital value chain - not delegated solely to front-facing platforms.* (Policy_demands (unknown))
>
> *The Commission should clarify in the guidelines that all entities enabling access to or interaction with online environments used by children bear proportionate, enforceable obligations to protect child users.* (Policy_demands (unknown))
>
> *Yet device manufacturers, telecom providers, and edtech platforms also play a significant role in children's access to and experience of digital services — and must share responsibility for risk mitigation.* (CONCLUSION & POLICY DEMANDS (unknown))
>
> *To achieve a truly level playing field, it is essential to adopt a technology-neutral approach that promotes collaboration and consistency across the industry.* (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))
>
> *The Guidelines should define opportunities to enhance mechanisms for coordination between national Digital Services Coordinators when addressing cross-border child safety issues.* (STATEMENT (Digipeace (Digirauha ry)))
>
> **Digital Services Act - Draft Guidelines on the Protection of Minors Online (Aylo Freesites Ltd.).** Aylo Freesites Ltd. proposes close industry-regulator collaboration, including sharing technical expertise and implementation data, to enhance effective protection for minors.
>
> **Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)).** The Union of Entrepreneurs and Employers (ZPP) urges guidelines that foster interoperability and encourage shared responsibility among all ecosystem actors.

The guidelines should therefore incentivise interoperable solutions and shared responsibility among all actors.

Ten recommendations to the European Commission to really protect children online (unknown). The document calls for extending protective obligations to encompass device manufacturers, telecom companies, and edtech platforms, recognizing their key roles in children's digital experiences.

Yet device manufacturers, telecom providers, and edtech platforms also play a significant role in children's access to and experience of digital services — and must share responsibility for risk mitigation.

CONCLUSION & POLICY DEMANDS (unknown). This document underscores the necessity to broaden DSA obligations to all digital ecosystem players, and details specific expectations for devices, telecom services, and edtech platforms.

Yet device manufacturers, telecom providers, and edtech platforms also play a significant role in children's access to and experience of digital services — and must share responsibility for risk mitigation.

Policy_demands (unknown). The policy brief advocates for enforceable obligations across the digital value chain, emphasizing that child safety duties should not be limited to visible platforms but apply proportionately to all entities enabling online access.

The Commission should clarify in the guidelines that all entities enabling access to or interaction with online environments used by children bear proportionate, enforceable obligations to protect child users.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). ADIGITAL recommends a technology-neutral, collaborative industry approach to foster consistency, fairness, and innovation in DSA compliance for minors' protection.

To achieve a truly level playing field, it is essential to adopt a technology-neutral approach that promotes collaboration and consistency across the industry.

Feedback to the European Commission's consultation on the protection of minors guidelines under the Digital Services Act (AIR MEDIAS SAS). AIR MEDIAS SAS supports partnership between industry, regulators, and NGOs, highlighting their work with ARCOM and AFNOR to develop standards and social responsibility tools protecting minors.

To this end, we are working with industry players and authorities or bodies such as the Autorité de Régulation de la Communication Audiovisuelle et Numérique (ARCOM) and the Agence Française de Normalisation (AFNOR) to develop standards for the protection of minors, as well as actively contributing to social responsibility initiatives, such as experiments to verify the age of users of online platforms.

EUROPEAN CHILD SHIELD PLATFORM Protecting children from pornography (European Child Shield Platform). The European Child Shield Platform highlights the need for reinforced cooperation among governments, internet infrastructure players, and civil society to combat online threats to minors.

Enhance cooperation between governments, internet servers and civil society associations, including children, parents and family associations

STATEMENT (Digipeace (Digirauha ry)). Digipeace advocates for enhanced cross-border coordination among national Digital Services Coordinators to address transnational issues of child safety.

The Guidelines should define opportunities to enhance mechanisms for coordination between national Digital Services Coordinators when addressing cross-border child safety issues.

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 (European Commission).

The European Commission recommends ongoing exchange of good practices and technological solutions among platforms, authorities, and stakeholders to raise the level of minors' privacy and security.

Exchanging between platforms and providers, as well as with Digital Services Coordinators, trusted flaggers, civil society organisations and other relevant stakeholders, good practices and technological solutions that are aimed at ensuring a high level of privacy, safety and security for minors.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). The Media Board urges coordinated action between Digital Services Coordinators and media regulators, aiming for harmonized procedures that ensure effective protection for minors.

iven the existing legal framework for minor protection under the Audiovisual Media Services Directive (AVMSD)5, in parallel to the new Digital Services Act (DSA), we believe that only a coordinated and complementary action among DSCs and media regulators as competent authorities for minor protection can provide a truly safe, secure and privacy friendly environment for users that are minor

How independent Audience Measurement Supports Minors' Online Safety Objectives (Audience Measurement Coalition). The Audience Measurement Coalition calls for stronger obligations for all ecosystem actors to participate in independent audience measurement, linking it to minors' safety objectives.

We recommend more defined and stronger obligations on all parties in the media ecosystems to participate in cross media audience measurement.

1.14.2 Standards and Technical Interoperability

The category 'Standards and Technical Interoperability' reflects a strong consensus across stakeholders on the necessity for harmonized technical standards and interoperable systems to protect children online under the EU Digital Services Act (DSA). Many submissions stress the adoption of official standards, notably CWA 18016 based on IEEE 2089, to ensure consistent age-appropriate digital services and effective protection measures across all platforms and devices. A recurring theme is the importance of cross-platform and cross-device interoperability—for example, ensuring parental controls and guardian tools function seamlessly across operating systems and devices to prevent gaps in protection. Technical recommendations include open APIs, standardized data formats, and real-time data access for middleware and age verification, along with certified, industry-sanctioned tools to simplify compliance and create a level playing field. Some contributions recognize challenges to implementing interoperable solutions, such as those with digital identity schemes, highlighting issues of trust, usability, accessibility, and current lack of technical alignment. There is also forward-looking support for EU-wide digital identity frameworks, provided they remain optional and user-centric.

Standards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA. (COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe))

Harmonised application: The guidelines should be applied in a harmonised and standardised way across all platforms used by children to ensure a consistent approach to protecting children's privacy, safety and security. (Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group))

It would provide a centralised device level approach to age assurance through which a service can request a user provide their age credentials, together with sufficient metadata for services to confirm they are appropriate. (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA. (Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe))

Some deliberative systems allow users to integrate, fork, or remix tools across platforms and communities. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

It is also a concern that, as regards the interoperability of guardian tools, many are not interoperable across different operating systems at the moment. (EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online))

Avaaz submission to the EU consultation on Article 28 Guidelines to Protect Children's Privacy, Safety, and Security (Avaaz). Advocates for industry-standard, cross-platform coordination to enable uniform protective interventions for minors across multiple services.

Implementing coordinated intervention systems that trigger across multiple platforms when concerning usage patterns are detected, ensuring comprehensive protection rather than platform-specific limitations.

Public consultation on 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 (Coimisiún na Meán). Highlights the absence of explicit reference to interoperability in the draft guidelines, recommending that the guidelines address how interoperable measures enhance their effectiveness.

An Coimisiun notes that the draft guidelines do not appear to reference interoperability of measures and the attendant point that how measures are combined and interact can be a contributing factor to their effectiveness.

Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)). Recommends official endorsement of certified, interoperable tools for age verification and moderation to lower compliance costs and standardize industry practices.

Promote access to certified, standardised tools: Official endorsement or support of interoperable tools for age verification and moderation can reduce compliance costs and level the playing field.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Emphasizes the value of interoperable, remixable tools in deliberative systems to foster collaborative engagement across communities and platforms.

Some deliberative systems allow users to integrate, fork, or remix tools across platforms and communities.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Calls for mandatory interoperability, data portability, and open protocols to support middleware and ensure user-centered digital ecosystems.

To ensure equitable, user-centered digital ecosystems, policymakers should enact legislation that requires dominant platforms to support certified middleware providers through open APIs, standardized data formats, and real-time data access.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Encourages adoption of formally recognized standards such as CWA 18016 to underpin protections for children under the DSA.

tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Urges integration of harmonized and technology-neutral industry solutions into DSA measures to create consistent protection and a level playing field.

Hence, when it comes to protection of minors, we believe that a key objective for the guidelines should be to establish a level-playing field across the ecosystem.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Proposes an Interoperability Principle based on a centralized, device-level approach to age assurance, with explicit recognition of operating system and app store roles.

It would provide a centralised device level approach to age assurance through which a service can request a user provide their age credentials, together with sufficient metadata for services to confirm they are appropriate.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Warns that current guardian tools lack interoperability across different operating systems, limiting parental control functionality.

For example, a parent with an Android device can't access the parental controls of a child using an iPhone.

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Recommends adopting CWA 18016 under Article 44 DSA to provide a standards-based framework for age-appropriate services.

CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

The "Segregate-and-Suppress" Approach to Regulating Child Safety Online (unknown). Notes significant real-world challenges with digital identity solutions including interoperability, accessibility, and trust, as seen in US state mobile IDs.

Currently, 13 states offer mobile driver's licenses, a type of digital ID, and have faced challenges such as interoperability, accessibility, usability, and trust").

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Highlights the importance of adopting CWA 18016 for age-appropriate service design per Article 44 DSA.

tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Urges the integration of CWA 18016 standards under the DSA for consistent digital services tailored to children.

Standards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom). Encourages platforms to ensure compatibility with interoperable and centralized digital parenting tools.

encouragement des plateformes à être compatibles avec les outils interopérables et centralisés pour les tuteurs.

Draft Guidelines under Article 28(1) of the Digital Services Act: Ensuring a High Level of Privacy, Safety and Security for Minors Online (Thorn). Emphasizes interoperability with national safer internet centers, law enforcement reporting, and adoption of CWA 18016 standards under Article 44 DSA.

Ensure interoperability with national Safer Internet Centres and law enforcement reporting protocols.

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Advocates for harmonized, standardized application of guidelines and interoperable guardian tools across all platforms, devices, and search engines children use.

Harmonised application: The guidelines should be applied in a harmonised and standardised way across all platforms used by children to ensure a consistent approach to protecting children's privacy, safety and security.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Supports development of trustworthy, optional, and interoperable EU-wide digital identity solutions for child protection.

In addition, we support the development of EU-wide solutions, such as the EU's Digital Identity Wallet, provided they remain optional, interoperable, and grounded in user trust.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Stresses the necessity of standards like CWA 18016 for age-appropriate design under the DSA.

Standards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Argues that adopting standards such as CWA 18016 is crucial for protecting children's online rights under the DSA.

tandards, such as the CWA 18016 on 'Age Appropriate digital services framework' based on IEEE 2089, also have a critical role to play and must be adopted under Article 44 of the DSA.

1.14.3 Guidance and Implementation Support

This category focuses on the critical role of clear, harmonized, and adaptable guidance for digital platforms to ensure effective interoperability and compliance with regulatory standards. Key insights emphasize the necessity for EU-level guidance to prevent fragmentation, particularly in child online safety, ensuring consistency across member states and reducing burdens on providers. There is also a strong call for guidance that acknowledges overlaps between various EU regulations (such as GDPR, AVMSD, and AI Act), offering practical support for platforms navigating complex requirements. Beyond regulatory coherence, the insights stress the importance of adaptability and localization—deliberative and safety-enhancing technologies must be modifiable to fit different cultural and social contexts to be truly inclusive and effective. Technical adaptation and external guidance are seen as vital, especially for legacy platforms revising their systems to meet new standards.

Strong, clear EU-level guidance is essential to discourage national deviations and support a consistent child safety framework across the EU. (Protecting children online: response to the draft guidance (DIGITALEUROPE))

We encourage the Commission to clarify that the "Guidelines" should be applied EU-wide and that Member States should avoid introducing their own measures. (Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland))

While the Guidelines aim to provide clarification within the scope of Article 28 of the Digital Services Act (DSA), they fall short in addressing the broader need for guidance on how online service providers should navigate overlapping EU regulatory frameworks. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

To be inclusive and effective, deliberative tools must be adaptable to different cultural, linguistic, and ethical contexts. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

For legacy media and platforms that children use, a challenge is the speed and scope of compliance with these guidelines. (IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)))

Fragmentation creates legal uncertainty, imposes disproportionate compliance burdens on providers and ultimately undermines child protection. (Protecting children online: response to the draft guidance (DIGITALEUROPE))

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Advocates for the adaptability and localization of technology governance frameworks, ensuring deliberative tools reflect local values and cultural contexts for inclusivity and effectiveness.

Communities should be able to modify or translate systems to reflect local norms, values, and governance needs-ensuring relevance across settings.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Highlights the need for regulatory guidance that addresses intersections with overlapping EU frameworks, helping platforms interpret and implement multiple compliance obligations consistently.

While the Guidelines aim to provide clarification within the scope of Article 28 of the Digital Services Act (DSA), they fall short in addressing the broader need for guidance on how online service providers should navigate overlapping EU regulatory frameworks.

Protecting children online: response to the draft guidance (DIGITALEUROPE). Calls for strong, EU-level guidance to prevent national divergence and ensure harmonized implementation of child safety measures across the single market, avoiding fragmentation.

Strong, clear EU-level guidance is essential to discourage national deviations and support a consistent child safety framework across the EU.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). Emphasizes challenges for legacy platforms in achieving compliance, underlining the importance of external guidance and substantial technical adaptation to meet child protection and ethical design standards.

Implementing robust age assurance, revising recommender systems, and embedding ethical design may require significant technical adaptation and external guidance.

Technology Ireland submission to the targeted public consultation on the protection of minors "Guidelines" under the Digital Services Act (Technology Ireland). Supports unified, EU-wide application of guidelines to reinforce harmonization in child safety requirements, warning against national deviations and highlighting the risk of regulatory overlap.

We encourage the Commission to clarify that the "Guidelines" should be applied EU-wide and that Member States should avoid introducing their own measures.

1.14.4 Legal and Regulatory Alignment

The key knowledge embedded in the category 'Legal and Regulatory Alignment' under Interoperability, Standards, and Ecosystem Responsibilities focuses on fostering legal clarity, harmonization, and coherence across the European Union's regulatory landscape, particularly for the protection of minors online. Insights from various stakeholders emphasize the importance of developing a unified European framework that clarifies the interplay between the Digital Services Act (DSA) and other relevant EU directives and regulations (such as the AVMSD, GDPR, and the European Digital Identity Regulation), to avoid legal fragmentation and insecurity for online platforms and enterprises. A recurring theme is the necessity to prevent divergent national rules that could undermine the single market, instead advocating for a consistent set of principles and compliance mechanisms that member states and platforms must follow. Contributions stress the significance of providing clear guidelines to delineate legal overlaps, especially in areas like age verification and parental controls, and ensuring the primacy of EU-level regulation. Some documents also highlight collaborative efforts among Member States and the European Commission to coordinate strategies and avoid duplicated or conflicting obligations.

Developing a European reference framework to ensure legal clarity and consistent treatment across Member States, while preventing circumvention. (Contribution Guidelines art 28 DSA (Respect Zone))

Ensure coherence across legal frameworks: The guidelines must avoid duplication and clearly articulate how they complement other EU rules, such as the Audiovisual Media Services Directive. (Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)))

Ce document constitue une référence utile pour garantir une mise en conformité cohérente dans l'ensemble de l'Union. (Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM))

The Guidelines should harmonize rules at EU level, providing consistent principles that applies across all online platforms. (Position of Polish Confederation Lewiatan on Commission's consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan))

To address the lack of clarity for online service providers, the Guidelines should clarify the relationship between different EU regulatory frameworks, including the DSA, Audiovisual Media Services Directive (AVMSD), General Data Protection Regulation (GDPR), and European Digital Identity Regulation. (Position of Polish Confederation Lewiatan on Commission's consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan))

A dedicated task force at the Ministry of Digital Governance was established to coordinate these proposals and engage with EU counterparts to prevent fragmentation across Member States. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Ce document constitue une référence utile pour garantir une mise en conformité cohérente dans l'ensemble de l'Union. (Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM))

A défaut, cela pourrait fragiliser le marché unique, en imposant aux acteurs, y compris les fabricants de terminaux, de s'adapter à des exigences divergentes selon le pays. (Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM))

A dedicated task force at the Ministry of Digital Governance was established to coordinate these proposals and engage with EU counterparts to prevent fragmentation across Member States. (Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance))

Contribution Guidelines art 28 DSA (Respect Zone). Proposes a European reference framework to secure legal clarity and a uniform approach across Member States, helping prevent circumvention of rules.

Union of Entrepreneurs and Employers (ZPP) Position Paper on Draft Article 28 DSA Guidelines (Union of Entrepreneurs and Employers (ZPP)). Advocates for coherence and non-duplication across legal frameworks, urging guidelines to articulate their relationship with existing EU rules like AVMSD.

Ensure coherence across legal frameworks: The guidelines must avoid duplication and clearly articulate how they complement other EU rules, such as the Audiovisual Media Services Directive.

Réponse de l'AFNUM à la consultation publique de la Commission européenne sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du DSA (AFNUM). Calls for harmonization of online protection measures for minors, underscoring the risk of market fragmentation and the need for standards compatible with the European DSA framework.

En évitant une fragmentation réglementaire, il permet de limiter l'insécurité juridique pour les entreprises tout en préservant un niveau élevé de protection des publics fragiles et vulnérables.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Highlights the unresolved regulatory ambiguity for service providers due to overlapping EU rules, recommending the guidelines clarify interrelations between key frameworks such as DSA, AVMSD, GDPR, and the AI Act.

guidelines should provide the necessary clarity on the interlinks and overlaps between the DSA and the Audiovisual Media Services Directive (AVMSD); between the DSA and the General Data Protection Regulation (GDPR) and between the DSA and the AI Act.

Position of Polish Confederation Lewiatan on Commission's consultation on the guidelines on protection of minors online under the Digital Services Act (Polish Confederation Lewiatan). Emphasizes harmonizing EU-level rules for minors' online protection, clarifying overlaps between the DSA and other frameworks, and asserting EU law's primacy over national initiatives.

To address the lack of clarity for online service providers, the Guidelines should clarify the relationship between different EU regulatory frameworks, including the DSA, Audiovisual Media Services Directive (AVMSD), General Data Protection Regulation (GDPR), and European Digital Identity Regulation.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Describes national coordination measures and stresses the importance of avoiding regulatory fragmentation through collaborative implementation under the DSA.

A dedicated task force at the Ministry of Digital Governance was established to coordinate these proposals and engage with EU counterparts to prevent fragmentation across Member States.

1.14.5 Competition and User Empowerment

This category highlights the importance of enforcing competition, interoperability, and uniform standards across digital platforms to empower users and foster the emergence of prosocial alternatives. The collection emphasizes that dominant platforms should be required to support open APIs, data portability, and interoperability, which would enable middleware services that give users greater control and choice, reducing dependence on monopolistic 'walled gardens.' Enhancing antitrust enforcement and removing barriers to entry can help smaller and prosocial platforms compete, while open standards ensure users can switch services and customize experiences without losing data or protections. The risks of fragmentation and inconsistent standards are also acknowledged, underscoring the need for harmonized, ecosystem-wide rules—particularly when it comes to safeguarding minors online. Within DSA compliance and youth protection, there is a call for a level playing field where all platforms (including social media, app stores, and OS providers) are subject to the same requirements and standards, which ensures cohesive safeguards and prevents some platforms from evading obligations. Recognizing the pivotal roles of operating systems and app stores, particularly regarding data portability, is stressed to maintain fairness and usability for all users, especially vulnerable populations.

Data sovereignty, portability, and interoperability are interrelated principles that define who controls digital data, how it moves, and how systems communicate. Together, they form the foundation for a more democratic, user-centered, and prosocial digital ecosystem. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Enforcing competition, antitrust, and anti-monopoly laws can open space for prosocial alternatives to emerge and thrive by leveling the playing field. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

to be effective, any measures foreseen by the guidelines should incorporate EU and industry-wide solutions whereby all platforms are held to the same consistent standard. (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))

By mandating open protocols and data portability, policymakers can help prevent monopolistic "walled gardens" and support smaller, prosocial platforms prioritizing ethical design and user well-being. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute))

Ensuring equitable access to APIs and infrastructure, maintaining platform neutrality, and implementing regulations, such as anti-bundling measures, are crucial for promoting competition and innovation. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

if the whole platform industry is held to the same standards and works together to provide safe, age-appropriate experiences, this would help young people avoid platforms that are not as safe as those that have invested in age-appropriate protections and experiences. (ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital))

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Advocates for mandating interoperability, open APIs, and data portability to break down monopolistic barriers, foster competition, and enable middleware that

empowers users and supports prosocial design, emphasizing the role of antitrust and policy in creating a user-centered digital ecosystem.

Data sovereignty, portability, and interoperability are interrelated principles that define who controls digital data, how it moves, and how systems communicate. Together, they form the foundation for a more democratic, user-centered, and prosocial digital ecosystem.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Focuses on the need for leveling the playing field through fair access, structural separation, and anti-bundling to allow ethical and prosocial platforms to emerge, while warning of risks like market fragmentation and the necessity of complementary prosocial standards.

Enforcing competition, antitrust, and anti-monopoly laws can open space for prosocial alternatives to emerge and thrive by leveling the playing field.

Meta Platforms Ireland Ltd. Response to EC Consultation on the guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Art. 28 DSA (Meta Platforms Ireland Ltd.). Stresses the objective of ensuring regulatory guidelines apply evenly across all online platforms under the DSA to avoid unfairly targeting social media and to maintain a consistent approach to user protection.

A key objective for the Guidelines should be to establish a level-playing field across the ecosystem of online platforms.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT (Adigital). Calls for harmonized, EU- and industry-wide standards for child safety and platform obligations, to ensure consistency and a level playing field, emphasizing the value of uniform protections for vulnerable users.

to be effective, any measures foreseen by the guidelines should incorporate EU and industry-wide solutions whereby all platforms are held to the same consistent standard.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Highlights the crucial responsibilities of operating systems and app stores, in line with the Digital Markets Act, to enable seamless age data portability and consistently apply user empowerment measures.

Explicitly recognize the central role of OS and app stores and their obligations under the Digital Markets Act in facilitating all users to port their age data through upstream signals;

1.14.6 Miscellaneous

1.15 Advertising, Commercial Practices, and Profiling

The most compelling theme emerging across this category is the shared priority of shielding minors from manipulative and data-driven advertising and commercial practices, with a “broad consensus on the need for stricter controls or outright bans on personalized or profiled advertising to minors.” Regulatory frameworks, risk-based safeguards, and platform responsibilities all converge on strengthening protections against profiling, covert marketing, and exploitative monetization tactics such as loot boxes and dark patterns. Substantial attention is paid to reinforcing both content standards and the demarcation between advertising and other content, especially given children's unique vulnerabilities and limited commercial literacy. Transparency and clear disclosure—tailored to minors’ developmental levels—are consistently emphasized, particularly for influencer marketing, virtual currencies, and AI-driven advertising. Self-regulatory and multi-stakeholder approaches gain support, but are paired with calls for robust regulatory backstops: for instance, “explicit safeguards for particularly risky product categories” and requirements for platforms to facilitate and enforce age-appropriate disclosures. Proposals highlight the need for harmonized, flexible frameworks that foster positive alternatives in monetization and advertising, while actively excluding exploitative practices and maintaining user control. Across all sub-categories, dominant trends include the focus on future-proofing rules

to address emerging digital challenges, harmonizing regulations with sectoral codes, and ensuring children's best interests consistently override commercial incentives.

1.15.1 Legal, Regulatory, and Compliance Frameworks

The category 'Advertising, Commercial Practices, and Profiling >> Legal, Regulatory, and Compliance Frameworks' encompasses a range of insights centered around regulatory measures designed to protect minors from targeted advertising, profiling, and potentially manipulative commercial practices online. There is broad consensus on the need for stricter controls or outright bans on personalized or profiled advertising to minors, with several stakeholders advocating for extending existing protections beyond current frameworks, such as those provided by the Digital Services Act (DSA). Notably, some contributions stress the importance of harmonizing these regulatory changes with established sector-specific codes or frameworks, ensuring that measures do not inadvertently limit non-commercial, public interest communications or result in conflicting obligations for platforms. The documents reveal a nuanced debate regarding definitions (e.g., what constitutes 'virtual currency'), the applicability and proportionality of bans (particularly regarding in-game content or supportive non-profit messaging), and the risk of over-prescriptiveness in regulatory language. Concerns are also raised about safeguarding sectoral communications (like lotteries or broadcasters) from being inappropriately categorized as harmful advertising. Recommendations include the adoption of risk-based and proportionate approaches, greater reliance on self-regulatory codes where robust, and sectoral action in cases where platforms adopt aggressive data-driven advertising models targeting children.

> *Sie betonen, dass es eines erweiterten Schutzes der kommerziellen Personalisierung im digitalen Raum bedürfe, da der bisherige Schutzrahmen durch den Digital-Service-Act (DSA) lediglich die Gruppe der Minderjährigen umfasse.* (TOP 21 Verbot von Tracking, Verhaltensanalysen und Profilbildung zu Werbezwecken (personalisierter Werbung) (Verbraucherschutzministerkonferenz))

> *Schutz und Kontrolle personalisierter Werbung bei Minderjährigen konsequent umzusetzen bis hin zu Verboten in Einzelfällen.* (Stellungnahme zur öffentlichen EU Konsultation: Leitlinien der Kommission für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre und Sicherheit für Minderjährige im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022 / 2065 (Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg))

> *The section of the Guidelines addressing commercial practices (Section 6.6), including marketing and advertising directed at minors, takes a very prescriptive tone.* (Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap))

> *If any specific practices related to how an in-game currency is used or is offered in a particular game is found to be misleading or aggressive, then those practices would already be prohibited under existing consumer law; however, a blanket prohibition against the use of in-game currency is not a proportionate measure and is not an appropriate recommendation for the Commission to make as part of the Guidelines - particularly when the economic impact that such a recommendation would have on the European digital single market has not been established through a robust assessment.* (Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE))

> *Any other interpretation of "virtual currency", or any implication that the exchange of a virtual item for an in-game virtual currency is an "economic transaction", would raise significant legal uncertainty and contradict well-established law.* (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

> *Lastly, we wish to highlight that national self-regulatory advertising codes, many of which are based on the International Chamber of Commerce's (ICC) Advertising and Marketing Code, already have their definition of "marketing and communication of products or services that can have an adverse impact on their privacy, safety and security" (lines 641-642).* (AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)))

TOP 21 Verbot von Tracking, Verhaltensanalysen und Profilbildung zu Werbezwecken (personalisierter Werbung) (Verbraucherschutzministerkonferenz). Calls for expanding protections and stricter monitoring of personalized advertising toward all users, not just minors, highlighting perceived gaps in the current DSA framework.

Sie betonen, dass es eines erweiterten Schutzes der kommerziellen Personalisierung im digitalen Raum bedürfe, da der bisherige Schutzrahmen durch den Digital-Service-Act (DSA) lediglich die Gruppe der Minderjährigen umfasse.

Stellungnahme zur öffentlichen EU Konsultation: Leitlinien der Kommission für Maßnahmen zur Gewährleistung eines hohen Maßes an Privatsphäre und Sicherheit für Minderjährige im Internet gemäß Artikel 28 Absatz 4 der Verordnung (EU) 2022 / 2065 (Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg). Advocates for the strict implementation and, where necessary, prohibition of personalized advertising to minors to ensure effective protection and privacy.

Schutz und Kontrolle personalisierter Werbung bei Minderjährigen konsequent umzusetzen bis hin zu Verboten in Einzelfällen.

CHILDREN'S LIVES WITH SOCIAL MEDIA (Børns Vilkår). Highlights the pervasive influence of influencer marketing on children's consumption habits and calls for increased regulation to shield minors.

Influencers affect children's consumption; many children want to buy products that influencers advertise.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). Urges clarification on the definition of 'virtual currency' in the DSA Guidelines, explicitly excluding in-game currencies from the scope of financial regulations.

The Guidelines should ensure that the use of "virtual currencies" in this context is limited to "virtual currency" as defined in Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on anti- money-laundering mechanisms such that it excludes "in-game currencies" utilised in video games.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Emphasizes proportionate regulation of in-game currencies and design features, and opposes blanket prohibitions in the context of minor protection guidelines.

The general prohibition of certain design features does not adhere to the General Principles set out in the Guidelines and advances an incorrect legal interpretation as regards the legal classification of in-game currencies.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Warns against unintended consequences of advertising bans by noting these may also prevent non-commercial organizations from communicating supportive messages to children.

Bris would like to remind the Commission that the prohibition in Article 28.2 has had the unintended consequence of also preventing non-commercial actors-such as NGOs and public authorities-from directing advertising toward children, based on profiling.

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Cautions that overly prescriptive or duplicative guideline requirements may create conflicts with existing EU law, especially regarding the regulation of advertising to minors.

Avoid prescriptive requirements that duplicate or conflict with existing EU legislation on data protection, commercial practices, and consumer rights;

Ecommerce Europe's reply to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Ecommerce Europe). Acknowledges the need for sector-specific regulation in cases where platforms employ data-driven models targeting minors, to better safeguard this demographic.

We understand that sectoral regulatory action might need to be taken in those cases.

The European Lotteries' Response to Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act (The European Lotteries). Requests that institutional and socially beneficial communications from lotteries are not misclassified as gambling advertising within DSA guidelines.

Such communications should not be confused with gambling advertising and should be safeguarded in the Guidelines to avoid undermining the social mission of lotteries.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). Promotes the idea that self-regulatory advertising codes can serve as effective standards for online platforms in meeting DSA requirements regarding minors.

Hence, these Codes could in fact become the de facto standard to which online platform providers can comply with the guidelines.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). References AVMSD obligations for commercial communications on video-sharing platforms and advocates additional restrictions on product placement aimed at minors.

Art 28b(3)b) including and applying in the terms and conditions of the video-sharing platform services the requirements set out in Article 9(1) for audiovisual commercial communications that are not marketed, sold or arranged by the video-sharing platform providers

Snap's response to the Public Consultation on the Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Article 28(4) of the Digital Services Act) (Snap). Critiques overly rigid or inflexible obligations in the DSA Guidelines, advocating for flexible, risk-based approaches to the regulation of advertising to minors.

The section of the Guidelines addressing commercial practices (Section 6.6), including marketing and advertising directed at minors, takes a very prescriptive tone.

1.15.2 Advertising Standards and Content

The key insights of the category 'Advertising Standards and Content' emphasize establishing robust and comprehensive protections for minors in digital advertising environments. Documents highlight the need for responsible marketing and advertising policies, both in terms of content (quality, ethics, legality) and volume (frequency, intensity of exposure). There is a consistent call to expand definitions of harmful marketing, considering not just overtly unethical ads, but also subtler impacts such as excessive quantity and the use of manipulative techniques like neuromarketing and emotional analytics. Stakeholders urge the incorporation of age-appropriate standards, clearer distinction between advertisements and other types of content, and specific prohibitions (e.g., product placement in children's programming). Recommendations include recognition and support for advertising industry self-regulation, robust risk assessment procedures, and explicit safeguards for particularly risky product categories (e.g., alcohol, tobacco, gambling). Additionally, documents address emerging digital challenges such as sharenting and child influencers, calling for clearer rules in these domains and stronger platform accountability.

Have a responsible marketing and advertising policy in place that does not allow harmful, both to the mental and physical health of the child, unethical and unlawful advertising to, for or by minors. (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))

Given the well-established nature of the self-regulatory advertising system and the role it plays in protecting minors from unethical and unlawful advertising practices, we believe it would be appropriate to recognise it in Section 6.6 of the draft guidelines. (AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)))

consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child

influencers. (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown))

These self-regulatory frameworks, built on shared responsibility and transparency, have proven effective. (WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers))

We have processes in place across our markets to approve new designs, campaigns and products to ensure they comply with socially responsible rules and those relating to youth appeal. (Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act Allwyn submission (Allwyn))

consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers. (Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown))

UNICEF Sweden's comments on the protection of minors guidelines under the Digital Services Act (UNICEF Sweden). UNICEF Sweden urges strengthening guidelines to better protect children by limiting ad frequency, addressing both mental and physical health impacts, and expanding the definition of harmful marketing.

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Eurochild advocates for responsible marketing policies that prohibit harmful, unethical, and unlawful advertising to, for, or by minors and encourage age-appropriate campaigns and better security measures.

Have a responsible marketing and advertising policy in place that does not allow harmful, both to the mental and physical health of the child, unethical and unlawful advertising to, for or by minors.

WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers). The World Federation of Advertisers emphasizes the importance of promoting global standards for age-gating and safeguarding minors from online alcohol advertisements.

We recommend that the European Commission recognise and promote these global standards and the important steps that have been taken to effectively protect minors from seeing alcohol ads online.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). This document stresses the necessity for digital platforms to clearly separate news, personal content, and advertisements to prevent confusion and maintain trust in journalism.

Confusion from mixing ads and personal content with news, making it hard to distinguish journalism from propaganda.

Media Board's submission to the European Commission's targeted public consultation on the draft guidelines on protection of minors under the Digital Services Act (European Board for Media Services). The European Board for Media Services recommends stricter controls on VSP commercial communications, including bans on subliminal techniques and product placements in children's programming.

shall not use subliminal techniques

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Bris highlights the need for guidelines to tackle not only the quality but also the quantity of advertising directed at children, considering cumulative impact even within ethical boundaries.

Bris finds that the guidelines lack a focus on the impact that advertising-even when it falls within ethical boundaries-can have on children.

Draft Guidelines on the Protection of Minors Online under Article 28(1) of the Digital Services Act Allwyn submission (Allwyn). Allwyn stresses a responsible approach to the promotion, advertising, and design of games, with a focus on marketing practices that do not appeal to underage audiences.

Responsible gaming approach to promotion, advertising, and design of games;

Missing Children Europe Submission Public Consultation on the guidelines on protection of minors online under the Digital Services Act (Missing Children Europe). Missing Children Europe calls for regulation of both type and volume of ads, banning manipulative marketing methods (neuromarketing, emotional analytics), and clarifies the need for guidance on influencers and sharenting.

c) Commercial practices: consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers.

STATEMENT (Digipeace (Digirauha ry)). Digipeace mirrors calls for addressing the type and quantity of advertising, banning immersive and analytic-driven techniques, and clarifying legal frameworks for digital child role models.

c) Commercial practices: consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). AIG underscores the effectiveness and importance of advertising self-regulation in protecting minors and suggests the DSA guidelines should acknowledge and support this system.

Given the well-established nature of the self-regulatory advertising system and the role it plays in protecting minors from unethical and unlawful advertising practices, we believe it would be appropriate to recognise it in Section 6.6 of the draft guidelines.

EL PAPEL DEL ENTORNO DIGITAL EN LA NORMALIZACIÓN DE LOS NUEVOS PRODUCTOS DE TABACO Y NICOTINA (Asociación Española Contra el Cáncer). The Asociación Española Contra el Cáncer recommends targeted measures for regulating digital tobacco/nicotine marketing, including restrictions on brand collaborations and event promotions aimed at youth.

Con este estudio, buscamos visibilizar el alcance de estas prácticas en nuestro país. Esta información resultará de gran relevancia a la hora de realizar análisis detallados y específicos de cada una de las estrategias estudiadas.

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 (European Commission). The European Commission advocates for the implementation of responsible marketing practices that protect minors across all age groups, with attention to adverse impacts and appropriate safeguards.

Have a responsible marketing and advertising policy in place that does not allow harmful, unethical and unlawful advertising (49) to, for or by min

EASA contribution to the European Commission's draft DSA Guidance on the Protection of minors (European Advertising Standards Alliance). EASA elaborates on the value of advertising self-regulation and calls for clear, consistent terminology in guidelines to align with the DSA, particularly for platforms' participation in ethical advertising practices.

Beyond the obligations for the platforms established under the DSA and the measures listed in the draft guidelines, the participation of online platforms in the ad self-regulatory system of the European Advertising Standards Alliance (EASA) is by itself a meaningful step, demonstrating their genuine commitment for improved protection of minors online.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). This document presses for clarifications and restrictions concerning commercial practices aimed at minors, especially in regard to innovative marketing techniques and the roles of sharenting and child influencers.

consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers.

IEEE_Response_15June2025__EU_Guidelines_Protection_of_Minors (Institute of Electrical and Electronics Engineers (IEEE) Standards Association (SA)). IEEE SA recommends all marketing targeting children be risk assessed, comply with age-appropriate standards, and be subject to change and auditing for ongoing compliance with children's rights.

Commercial practices must ensure all marketing and advertising aimed at children is risk assessed, amended according to the age-appropriate guidelines and subject to change control and configuration management practices, especially for compliance and auditing.

1.15.3 Data Use, Profiling, and Targeting

The category 'Data Use, Profiling, and Targeting' in the context of minors centers on the widespread call for prohibiting or severely restricting commercial profiling and targeted advertising to children online. Multiple contributions highlight regulatory gaps and urge for a broader ban that encompasses all forms of advertising, not only user-profile-based targeting. There is considerable emphasis on strengthening and clarifying restrictions within the Digital Services Act (DSA), including explicit limitations on behavioral data use, profiling, and AI-driven targeting practices, particularly for platforms providing services likely to reach minors. Some stakeholders support exceptions for responsible use of age-based signals to protect children from inappropriate content but oppose all exploitative or invasive commercial profiling. The importance of promoting privacy-respecting alternatives like contextual advertising, ensuring transparency, and considering feasibility and proportionality of data collection obligations is also discussed. Underpinning these proposals is a consistent reference to international child protection standards, such as the UNCRC, and a clear prioritization of the best interests of minors over commercial interests. Overall, the insights reveal a broad consensus that regulatory measures should be comprehensive and future-proof, focusing both on the prohibition of profiling-based advertising for minors and on transparency and data minimization in all commercial and recommendation practices involving minors' data. There are also innovative proposals for letting minors actively signal preferences, rather than relying on passive tracking, and for explicitly excluding certain AI-based profiling and recommendation systems from use with children.

Paragraph 2 prohibits providers of online platform from presenting advertisements on their interface based on profiling, as defined in Article 4, point (4), of Regulation (EU) 2016/679, 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. (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 (European Commission))

Profiling should not occur by default for minors. (Feedback DSA (unknown))

Ensure that there is no tracking-based advertising to minors. (PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)))

Our findings indicate that contextual targeting, when applied at the granularity of individual videos, can facilitate more precise micro-targeting than traditional behavioral methods. (Urgent Concerns Regarding Online Marketing to Children on Digital Streaming Platforms and the Adequacy of Current Regulations (Inria))

This approach respects their autonomy and privacy, while still allowing for personalization when desired. (Feedback DSA (unknown))

In light of the news media's essential role in bolstering democracy, EU institutions should take care to preserve and promote privacy-respecting revenue models for online media. (CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe))

Urgent Concerns Regarding Online Marketing to Children on Digital Streaming Platforms and the Adequacy of Current Regulations (Inria). Highlights that digital streaming platforms target children through placement-based advertising despite lacking direct profiling and urges the expansion of EU legal protections to ban all advertising to minors.

CS2023.pdf demonstrates that despite the absence of direct user profiling for child accounts, online streaming platforms enable highly targeted advertising to children.

Salminen contribution protection of minors (Aalto University). Stresses the need for clearer guidance on what counts as personalized or targeted advertising under the DSA to ensure uniform protection of minors.

To ensure the consistent application of Article 28(2), the Commission should provide clearer guidance on what constitutes as personalized advertisement in the context of the DSA, including how placement and segment-based strategies are to be treated under the regulation.

WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers). Supports the ban on profiling minors for advertising under the DSA, while allowing for responsible age-based targeting to exclude inappropriate content.

At the same time, we note that certain targeting practices, when used responsibly, can help protect minors by excluding them from content or ads that are not appropriate to them.

CDT Europe response to the public consultation for the draft Guidelines on the Online protection of Minors under Art.28 (Centre for Democracy and Technology Europe). Advocates for including contextual advertising as a privacy-respecting best practice in DSA guidelines and preserving non-intrusive commercial models.

One privacy-respecting alternative to profiling-based advertising that is often proposed is contextual advertising.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Calls for a ban on all tracking-based advertising and strict limitations on minors' data use by online platforms in the EU.

Ensure that there is no tracking-based advertising to minors.

EU Kids Online - Feedback on the Guidelines Pursuant to Article 28(4) DSA (Protection of Minors) (EU Kids Online). Notes that guidelines should address not just specific features but the underlying data-driven, exploitative business models affecting children.

The long list of requirements addresses the many features and functionalities that are currently problematic, but does not address the basic business model, which is data-invasive and commercially exploitative of children.

Digital Services Act Guidelines on Protection of minors (Art. 28(1)) (European Tech Alliance). Recommends that data collection and transparency obligations under the DSA be assessed for their balance between protection and operational feasibility, especially for platforms with unregistered users.

Recommendations related to data collection and transparency should be carefully assessed for both their protective value and their practical impact:

HOMO DIGITALIS CONTRIBUTION TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE DRAFT GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS (Homo Digitalis). Urges for default settings that expressly prevent data profiling and behavioral targeting of minors, especially by third-party ad tech and algorithmic systems.

Default settings should not only restrict interactions but also prevent data profiling and behavioural targeting-especially by third-party ad tech or algorithmic systems.

Feedback DSA (unknown). Advocates that profiling of minors should not be the default; instead, minors should actively indicate and update their interests, avoiding passive tracking.

Profiling should not occur by default for minors.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Warns against the use of AI for commercial profiling, targeting, or recommendations towards minors, including through conversational chatbots.

We strongly recommend that the Commission clarify that the use of AI for commercial profiling, targeting or recommendation – especially through seemingly conversational or advisory formats, such as commercial anthropomorphic chatbots – should be prohibited in services accessible to minors.

Contribution to the consultation on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the Digital Services Act (Ghent University, Law & Technology). Calls for a clear prohibition on using children's behavioral data for commercial purposes, emphasizing the best interests of the child over commercial motives.

In line with the best interests of the child, as set out in the UNCRC and explained in the General Comment No. 25 of the UN Committee on the Rights of the Child, commercial interests should not be prioritised over those of the child.

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 (European Commission). Defines the regulatory requirement that online platforms must not present profiling-based ads using personal data when they know with reasonable certainty the user is a minor.

Paragraph 2 prohibits providers of online platform from presenting advertisements on their interface based on profiling, as defined in Article 4, point (4), of Regulation (EU) 2016/679, 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.

Submission on the European Commission Art. 28 Guidelines (Leiden Law School, Leiden University). Highlights that the DSA guidelines should explicitly prohibit behavioral profiling of children for commercial purposes, not just behavioral advertising.

it is relevant that the Guidelines indicate that online commercial profiling of children is, in principle, contrary to the high level of privacy (and safety) that children deserve under Article 28 DSA, as well as the GDPR, in accordance with its Recitals 38 and 71.

INFORME DE LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO SOBRE EL DOCUMENTO "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" (Dirección General de Ordenación del Juego). Affirms the prohibition against online platforms using personal data profiling for ads when it's reasonably certain the recipient is a minor.

Los prestadores de plataformas en línea no presentarán anuncios en su interfaz basados en la elaboración de perfiles, tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679, mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor.

1.15.4 Protection from Harmful and Manipulative Practices

The insights within the category 'Protection from Harmful and Manipulative Practices' emphasize the need for robust regulations and clear guidelines to shield minors from various forms of commercial exploitation and manipulation in digital environments. Key points include preventing children's exposure to harmful or covert advertising, manipulative design techniques (such as loot boxes, dark patterns, emotional analytics, and neuromarketing), and ensuring a distinct separation between content and opportunities for purchases. Multiple

submissions underline the unique vulnerabilities of minors—including limited commercial literacy and the inability to critically assess advertising—necessitating strict safeguards and proactive measures from platforms. Stakeholders advocate for expanding legal and policy provisions to explicitly address emerging manipulative practices and to prioritize minors' safety, privacy, and security. Recommendations include banning certain high-risk advertising formats, maintaining minors' ability to use privacy tools (like ad blockers), and consulting with both children and guardians when developing and reviewing advertising policies. Techniques such as covert influencer marketing and immersive advertising are flagged as particularly problematic. Targeted protections are also recommended for new risks such as AI-driven nudges and the intersection with child influencers and 'sharenting.'

> *Ensure that minors are not exposed to marketing and communication of products or services that can have an adverse impact on their privacy, safety and security, including as identified in the provider's risk review.* (Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild))
>
> *We strongly support the guidelines that protect minors from economically exploitative commercial practices, including certain advertising practices to which they are particularly vulnerable.* (Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple))
>
> *Children may also not be able to distinguish between genuine content and advertising, making them more prone to covert commercial influence.* (PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)))
>
> *The Guidelines could benefit from more explicit references to industry practices that rely on real-time behavioural influence and manipulation.* (Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation))
>
> *pple has long championed efforts to rein in the excesses of a complex eco-system of websites, apps, social media companies, and data firms that track users online and harvest their personal information.* (Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple))
>
> *Ad Zeile 653: Das BMASGPK teilt die Auffassung der EK, dass für Kinder und Jugendliche keine virtuellen Zwischenwährungen zum Einsatz kommen sollten (Problem: fehlende Kostentransparenz, insbesondere für Minderjährige).* (Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)))

Eurochild contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act (Eurochild). Calls for stronger safeguards in the DSA to prevent children from being targeted by marketing that threatens their privacy or safety, and to address manipulative design and economic exploitation.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Supports guidelines to protect minors from economically exploitative commercial and advertising practices to which they are particularly vulnerable.

> *We strongly support the guidelines that protect minors from economically exploitative commercial practices, including certain advertising practices to which they are particularly vulnerable.*

Additional contribution (Collective Shout). Highlights the need to prevent the sale and advertising of child-like sex abuse dolls and explicit exploitation material on online platforms.

> *Instagram slammed for 'fuelling' the sale of child-like sex dolls: our investigations in the media.*

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Advocates for distinguishing between fair and manipulative commercial practices in the video games sector and for protecting minors from persuasive techniques leading to unintended purchases.

As an industry we are very committed to maintaining a high level of protection for minors.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Emphasizes the importance of enabling children to recognize advertising and avoid covert commercial influence by ensuring a clear distinction between content and ads.

Children may also not be able to distinguish between genuine content and advertising, making them more prone to covert commercial influence.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (5Rights Foundation). Recommends revising commercial practices to safeguard minors from aggressive ad targeting, neuromarketing, immersive ads, and addressing challenges with sharenting and child influencers.

c) Commercial practices: consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Suggests explicit inclusion of manipulative industry practices and calls for strengthened safeguards against profiling minors under the DSA.

For example, using time-limited offers during intense moments of gameplay (as referenced in footnote 55) is a well-documented dark pattern.

Not just users, but rights holders: realising the DSA's promise for children with the guidelines on article 28 (unknown). Stresses the need for commercial safeguards against exploitative advertising tactics, including emotional analytics, immersive ads, and practices targeting child influencers.

c) Commercial practices: consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers.

COFACE Families Europe submission to the European Commission targeted public consultation on the protection of minors guidelines under the Digital Services Act (COFACE Families Europe). Recommends responsible advertising for minors and clearer measures to prevent AI chatbot-driven data abuse and exploitation.

COFACE welcomes the inclusion of the provision on responsible marketing and advertising policy that does not allow harmful, unethical and unlawful advertising to, for or by minors.

Feedback DSA (unknown). Urges online platforms to prevent covert advertising targeting minors, such as inappropriate influencer endorsements.

Platforms must prevent covert advertising targeting minors, including product endorsements by influencers that do not comply with advertising rules.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). Stresses the importance of prioritizing online advertising protection for minors, highlighting industry codes to prevent harmful, unlawful, or exploitative content.

The advertising industry regards the protection of minors online as an important objective, both from a moral and legal perspective, and that it should be prioritised in a period of rapid technological advancement.

Contribution de l'Arcom à la consultation publique sur les lignes directrices relatives à la protection des mineurs en ligne dans le cadre du règlement sur les services numériques (Arcom).

Recommends platforms ensure a clear separation between content consumption and purchasing to protect minors' commercial safety.

l'Arcom suggère d'ajouter une exigence visant à faire respecter une séparation claire ou créer de la friction entre le visionnage du contenu et l'achat de produits.

Apple Response to the public consultation on the protection of minors guidelines under the Digital Services Act (Apple). Echoes strong support for guidelines that protect minors from economic and advertising exploitation, highlighting their increased vulnerability.

We strongly support the guidelines that protect minors from economically exploitative commercial practices, including certain advertising practices to which they are particularly vulnerable.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Advocates for preserving children's ability to avoid advertising exposure by supporting the use of adblockers and equivalent tools.

the ability to use a platform without being exposed to advertising – for instance through the use of adblockers or equivalent privacy-preserving tools – should be preserved and not be undermined by platform design or business models.

Comments of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection Art 28 DSA (Österreichisches Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)). Calls for banning loot boxes and similar manipulative gambling-like practices for minors and for wider protection from exploitative ads.

Aus Verbraucherperspektive sollten Loot Boxen, simuliertes Glücksspiel, Glücksräder und ähnliche Praktiken - zumindest für Minderjährige - auf Online Plattformen generell nicht zum Einsatz kommen.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Recommends prohibiting interactive ad formats like Playable Ads targeting children and pro-actively controlling advertising for adult-targeted 'nudify-apps' on youth-oriented platforms.

Playable Ads sind interaktive Werbeformate, bei denen Nutzer während der Nutzung einer App (z. B. während dem Schauen von Kurzvideos auf TikTok) eine verkürzte, spielbare Vorschau eines Spiels oder Produkts erleben können.

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 (European Commission). Identifies several consumer risks to minors online—including exposure to marketing risks, profiling, financial, and security risks—under the DSA.

Minors can also face risks as consumers in the digital economy: a. marketing risks (e.g. loot boxes, advergames.), b. commercial profiling risks (e.g. product placement or receiving advertisements intended for adults such as dating services), c. financial risks (e.g. fraud or spending large amounts of money on without the knowledge or consent of their guardians), d. security risks.

Greece's contribution to the open consultation on the European Commission's draft Guidelines on article 28 of the Digital Services Act (Hellenic Ministry of Digital Governance). Advocates for regularly reviewing advertising policies with stakeholders and specifically recommends prohibiting AI nudges towards commercial content for minors.

Ensure that minors are not exposed to the volume of advertising and commercial prompts that are detrimental to their safety.

Joint Statement on Article 28 Guidelines (5Rights Foundation). Calls for nuanced commercial practice regulations for children, including limits on ad volume, neuromarketing, and measures on influencer and sharenting issues.

c) Commercial practices: consider not only the quality and type of advertisements being presented to children but also its volume, ensure that minors are not exposed to practices that rely on

neuromarketing, emotional analytics and immersive advertising and clarify measures relating to cases of sharenting and child influencers.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Supports guidelines focusing on protecting minors from commercial exploitation, with specific reference to influencers, loot boxes, and manipulative practices.

We support the overall guideline that minors, particularly, need to be protected and have a right to be protected against commercial and economically exploitive practices.

Epic Games Response to European Commission Public Consultation Guidelines on protection of minors under the Digital Services Act (Article 28) (Epic Games). Stresses the need for transparency in commercial practices to prevent minors and other users from exploitative or accidental purchases within games.

We have designed our games to give players a fair and transparent in-game purchasing experience.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Highlights the importance of not exploiting minors' lack of commercial literacy, and supports restrictions on loot boxes and friction between content and purchasing.

Ensure that minors' lack of commercial literacy is not exploited by considering minors' age, vulnerabilities and limited capacity to engage critically with commercial practices on the platform and provide relevant support.

Position du groupe La Poste (La Poste). Summarizes national initiatives in France to adapt advertising messages for minors' maturity and to ensure their specific protection in commercial communications.

Les messages publicitaires soient adaptés à la maturité et à l'expérience des mineurs ;

1.15.5 Transparency and Disclosure

The category 'Transparency and Disclosure' in the context of advertising, commercial practices, and profiling, particularly for minors, emphasizes the necessity of clear, visible, and accessible disclosures regarding commercial content and advertising activities. Key insights from the documents highlight the importance of ensuring that disclosures are tailored to minors' developmental level, are consistently implemented across platforms, and that hidden or disguised advertising (such as undisclosed influencer marketing or AI-integrated ads) is strictly prohibited. Transparency about advertising placement, funding, and economic transactions (especially where virtual currencies are involved) is repeatedly underscored, along with measures enabling user and parental understanding and control. Several contributors stress the harmonization of disclosure standards, flexibility for age-appropriate design, and the avoidance of exploitative commercial practices aimed at children. There is also recognition of emerging challenges, such as AI-driven ads and virtual currencies that obscure true costs, necessitating additional safeguards. The importance of both the quality and quantity of commercial exposure to minors is raised, with calls for proactive, outcome-based approaches to disclosure. Recommendations span from specific technical requirements (e.g., clarity in ad libraries and in-game purchases) to broader policy suggestions for ongoing review and stakeholder consultation.

We favour clear disclosure requirements and safeguards to ensure minors' lack of commercial literacy is not exploited. (WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers))

For example, requiring platforms to be transparent in ad placement and funding and offering tools for users to understand and control ads are part of Safety by Design. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Ensure that minors are not exposed to hidden or disguised advertising, whether placed by the provider of the online platform or the users of the service (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 (European Commission))

Bris wishes to highlight the issue of advertising integrated into platforms' Al services. (Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris))

we recommend that the guidelines be strengthened by addressing not only the quality but also the quantity of commercial exposure to which children are subjected. (Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår))

The recommendation on clear and child appropriate declaration of commercial communication is too general to provide guidance on the matter. (Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency))

Urgent Concerns Regarding Online Marketing to Children on Digital Streaming Platforms and the Adequacy of Current Regulations (Inria). Argues for mandated ad library transparency, requiring explicit information about the use of placement-based advertising targeting minors.

WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers). Advocates for harmonised, clear commercial disclosure requirements and protection for minors from exploitative commercial practices.

We favour clear disclosure requirements and safeguards to ensure minors' lack of commercial literacy is not exploited.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion/Toda Peace Institute). Recommends platforms ensure transparency in ad placement and funding, with user tools for ad understanding as part of safety design.

For example, requiring platforms to be transparent in ad placement and funding and offering tools for users to understand and control ads are part of Safety by Design.

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Suggests transparency obligations on advertising and data monetization, and empowering users with ad controls for prosocial tech governance.

For example, requiring platforms to be transparent in ad placement and funding and offering tools for users to understand and control ads are part of Safety by Design.

Public consultation on the draft 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 Response from VIDEO GAMES EUROPE (VIDEO GAMES EUROPE). Calls for transparency in economic transactions involving minors, cautioning against the use of virtual currencies that may obscure costs.

Ensure transparency of economic transactions in an age-appropriate way and avoid techniques the use of intermediate virtual currencies, such as tokens or coins, that can be exchanged with real money and then used to buy other virtual items, which can have the effect of reducing transparency of economic transactions and may be misleading for minors, with reference to existing Union consumer law and guidance.

Bris comments on the European Commission's draft guidelines on measures to ensure a high level of privacy, safety and security of minors online pursuant to article 28 of regulation (EU) 2022/2065 (Bris). Highlights the risks of undisclosed, AI-driven advertising targeting children via chatbots and advocates for clear identification and disclosure.

It is currently the case that AI chatbots, in their conversations with children, may promote advertising without it being 1) clearly identified as advertising 2) disclosed as originating from a generative chatbot 3) based on minors data and behaviour.

ADIGITAL'S CONTRIBUTION TARGETED PUBLIC CONSULTATION ON THE PROTECTION OF MINORS GUIDELINES UNDER THE DIGITAL SERVICES ACT

(Adigital). Notes the need for platform-provided tools and policies ensuring commercial content transparency for minors, with particular focus on influencer product placement.

Subtle influencer product placement is fundamentally a creator's issue.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). Emphasizes outcome-based, flexible, and contextually child-friendly approaches to disclosures about advertising for minors.

And to accommodate these differences, we suggest an outcome-based approach to achieve the "child-friendly and accessible" objective described in the guidelines.

Børns Vilkårs Comments on the Commission's Draft Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (Børns Vilkår). Raises the issue of both the quality and cumulative volume of advertising exposure to children, calling for stronger guidelines.

The cumulative volume of advertising and commercial prompts can have significant effects on minors' well-being, even when individual instances meet legal and ethical standards.

ANMERKUNGEN UND FRAGEN ZU ART. 28 DSA-LEITLINIEN (Österreichisches Institut für angewandte Telekommunikation (ÖIAT)). Advocates for clear, comparable pricing information on digital content and in-game currencies to ensure cost transparency for minors.

Spieleanbieter müssten beim Kauf klare Informationen über den Preis einer Einheit der In- Game-Währung anbieten und beim Kauf mit In-Game-Währung über den Preis des digitalen Inhalts in realer Währung informiere

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 (European Commission). Sets out fundamental requirements for clear, visible, and child-friendly declarations of commercial communication, and regular review with stakeholder input.

Ensure that minors are not exposed to hidden or disguised advertising, whether placed by the provider of the online platform or the users of the service

EASA contribution to the European Commission's draft DSA Guidance on the Protection of minors (European Advertising Standards Alliance). Suggests refining guidelines by specifying 'undisclosed' influencer product placements as disguised commercial communications.

We therefore recommend inserting the word "undisclosed" before "product placements".

Vodafone Consultation Response to the European Commission on the Draft Guidelines under Article 28(4) of the Digital Services Act (Vodafone Group). Calls for further guidance on age-appropriate advertising transparency and labelling, especially for influencer and user-generated content.

We recommend the Commission develop further guidance on age-appropriate advertising transparency and labelling standards, especially in under 18 influencer and user-generated content.

TikTok response to public consultation on Article 28(4) DSA Guidelines (TikTok Technology Limited). Supports consistent implementation of disclosures across platforms and warns against virtual currencies that may mislead children.

ensuring declarations of commercial communications are used 'consistently throughout the service' (635-640) is a helpful benchmark; however, this is true for all users and it is arguably already required under EU law.

Feedback on the draft Commission guidelines on DSA article 28 (Swedish Agency for the Media). Proposes precise language, acknowledging that if influencer product placement is properly disclosed, it is not disguised commercial communication.

This should rather be phrased as "may include", as for example product placement by influencers could be disclosed properly and if so, is not disguised.

Response to Consultation on Guidelines under Art. 28(4) DSA (PEGI). Details recent PEGI Code updates ensuring fairness and transparency in in-app purchases, loot boxes, and virtual currency beyond legal requirements.

The 2023 update to the PEGI Code also included several commitments relating in-app purchases, loot boxes and virtual currency to ensure fairness and transparency, which go beyond legal what is required by law in relation to online purchases

Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency). Critiques general recommendations for clear, child-appropriate disclosure, emphasizing the complexity and contextual factors involved.

It's clear that designing a child appropriate disclosure is complex, and that several factors need to be considered, e.g., wording, placement, design including font, size, opacity, format, etc., and specific vulnerabilities of children.

1.15.6 Influencer and Platform Responsibilities

The insights in the category 'Influencer and Platform Responsibilities' center on the delineation and improvement of duties between influencers, online platforms, and industry stakeholders to protect minors from harmful, unethical, or unlawful advertising. There is broad support for collaborative, multi-stakeholder efforts—both regulatory and self-regulatory—to ensure responsible marketing practices, particularly the need for platforms to provide tools and policies for transparency, while creators bear primary disclosure responsibilities. Several documents emphasize that platforms should not serve as direct enforcers of all third-party commercial compliance, but must facilitate disclosure, enable reporting of violations, and act when necessary. A recurring theme is the call for influencer training, certification, and clearer labelling to enhance legal compliance and transparency, especially regarding commercial content targeting minors. Lastly, there is recognition that even with labelling, distinguishing commercial intent—particularly through influencers—remains difficult for children, thus requiring more precise guidelines and accessible disclosures to prevent commercial exploitation.

Thus content creators should be responsible for transparency, while platforms should provide the necessary tools and policies to enable it. (AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC))

provide the means to creators to disclose paid promotions; (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

We recommend that the Guidelines clarify that providers should ensure that they: (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

take appropriate enforcement action upon becoming aware of unlawful paid promotions. (Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited))

Commercial practices are already regulated (e.g., AVMSD, UCPD). Platforms should not be required to verify the compliance of third parties (like influencers) with these rules. (DOT Europe response1 (DOT Europe))

We recommend the Commission to provide more precise guidelines on how platforms can make sure that children are not exploited and exposed commercially. (European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children))

WFA response Targeted consultation Guidelines on the protection of minors under the Digital Services Act Supplementary statement (World Federation of Advertisers). This document promotes joint development of responsible marketing policies between platforms, advertisers, and stakeholders to restrict inappropriate advertising to minors, highlighting the value of existing self-regulatory efforts.

AMETIC's response to the Draft Guidelines for the Protection of Minors under Article 28 DSA (AMETIC). It emphasizes that content creators should be primarily responsible for transparency in commercial content, while platforms support this with necessary policies and tools.

Thus content creators should be responsible for transparency, while platforms should provide the necessary tools and policies to enable it.

DOT Europe response1 (DOT Europe). The response underscores that platforms should not be held accountable for verifying third-party compliance with existing commercial practice regulations.

Commercial practices are already regulated (e.g., AVMSD, UCPD). Platforms should not be required to verify the compliance of third parties (like influencers) with these rules.

Feedback DSA (unknown). This document suggests requiring influencers to declare their target audience and to demonstrate compliance with advertising and children's rights when addressing minors.

Influencers should indicate whether their content is targeted toward adults, minors, or both, and be held accountable to the respective advertising and content guidelines.

AIG RESPONSE TO THE COMMISSION'S GUIDELINES ON MEASURES TO ENSURE A HIGH LEVEL OF PRIVACY, SAFETY AND SECURITY FOR MINORS ONLINE PURSUANT TO ARTICLE 28(4) OF REGULATION 2022/2065 (13 MAY 2025) (Advertising Information Group (AIG)). It advocates for expanded influencer training and transparent disclosure rules, including certification programs to incentivize legal compliance and raise awareness of influencer marketing responsibilities.

For example, the German SRO (Deutscher Werberat) recently launched a 90 minute influencer online course, covering both German and European advertising laws, with the ultimate goal of increasing awareness of legal duties as well as transparency regarding influencer marketing.

Google_feedback_-_DSA_Art._28_draft_Guidelines (Google Ireland Limited). Google recommends clarifying platform responsibilities around undisclosed advertising, suggesting platforms should provide disclosure mechanisms, avenues for third-party reporting, and take enforcement actions, while also noting limitations in enforcing disclosure.

We recommend that the Guidelines clarify that providers should ensure that they:

European Commission's proposal for Guidelines under Article 28 of the Digital Services Act Save the Children feedback (Save the Children). Save the Children calls for more detailed guidelines to protect children from commercial exploitation, acknowledging the persistent challenge of identifying influencer-promoted commercial content despite labelling schemes.

We support that declaration of commercial communication is clearly visible, child-friendly and accessible (line 635), however, despite labelling schemes, it is difficult to discern commercial intent if a product is promoted by influencers.

1.15.7 Monetization and Commercial Mechanisms

The insights in the category 'Monetization and Commercial Mechanisms' focus on the design, risks, and governance of various monetization models used in digital technologies, with an emphasis on both prosocial and potentially exploitative practices, particularly as they affect children and minors. Several documents highlight the dangers of data extraction, advertising-driven incentives, loot boxes, gambling-like mechanisms, and opaque virtual currencies, especially for vulnerable populations such as minors. There is broad advocacy for default limits, increased transparency, and regulatory safeguards to prevent manipulative or non-transparent spending, including recommendations to disable in-app purchases and virtual currency transactions by default for children. Parallel to risk mitigation, attention is given to positive alternatives in tech design: prosocial approaches to monetization, such as subscriptions, pay-per-use, and cooperative models, which prioritize sustainable value delivery and eschew exploitative engagement or data use. Sustainable funding sources (public, private, and philanthropic) are identified as essential to scale such initiatives. The scope of commercial practices is also urged to expand, holding platforms accountable for their roles as de facto marketplaces and ensuring robust regulation not only covers advertising but the facilitation of transactions directly enabled by platform features. Finally, some regulatory bodies question the appropriate locus of these recommendations, emphasizing the need for coordination and clarity between overlapping legal frameworks.

Models with high potential for supporting prosocial outcomes-such as subscription-based, software-as-a-service (SaaS), licensing, and pay-per-use-focus on value delivery without exploiting user data or manipulating engagement. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

Minors are particularly vulnerable to impulsive decisions, manipulation, and financial harm. Minors typically do not possess the financial literacy required to make informed purchasing decisions. They may struggle to differentiate between virtual currency and real money or to understand the concept of recurring charges and cumulative costs. This can lead to unintended overspending. (PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)))

The Guidelines appropriately highlight the risks associated with exploitative monetisation tactics, such as loot boxes, other products with random or unpredictable outcomes or gambling-like features, intermediate virtual currencies, such as tokens or coins that can be exchanged with real money, and in-game purchases that are necessary to access core functionalities (lines 653-657 and 661-665). (Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation))

Some prosocial tech companies can utilize monetization models, such as subscription-based and pay-per-use, to remove ad-based incentives for divisive content. (Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute))

we recommend further demonstrating the existence of a clear link between the commercial practices addressed in Section 6.6. and their negative impact on minors' privacy, security and safety to emphasise their relevance in the context of the Guidelines. (Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation))

Social media services function as sophisticated, de facto marketplaces. (Contribution from medical professionals regarding the Draft Commission Guidelines on the Protection of Minors Online (Article 28 DSA) (Youth Smoking Prevention Foundation (Stichting Rookpreventie Jeugd); #vapenjouwkeuze))

Blueprint on Prosocial Tech Design Governance (Council on Technology and Social Cohesion with University of Notre Dame and Toda Peace Institute). Emphasizes the importance of prosocial monetization models that avoid data extraction and advertising, advocating for value-driven, sustainable funding and public/private investment to support positive tech outcomes.

Models with high potential for supporting prosocial outcomes-such as subscription-based, software-as-a-service (SaaS), licensing, and pay-per-use-focus on value delivery without exploiting user data or manipulating engagement.

PROTECTION OF MINORS ONLINE (Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband - vzbv)). Argues that minors are especially vulnerable to impulsive or unintended spending due to lack of financial literacy, calling for default deactivation of in-game purchases and establishment of clear spending limits.

Minors are particularly vulnerable to impulsive decisions, manipulation, and financial harm. Minors typically do not possess the financial literacy required to make informed purchasing decisions. They may struggle to differentiate between virtual currency and real money or to understand the concept of recurring charges and cumulative costs. This can lead to unintended overspending.

Feedback on the European Commission's Draft Guidelines on the Protection of Minors Online under Article 28(4) of the Digital Services Act (Working Group on Gaming and Regulation). Advocates for removing gambling-like and manipulative economic features for minors, emphasizing children's rights and preserving strong language on protecting against exploitative commercial practices.

In particular, the emphasis on removing gambling-like features for minors, including randomised reward mechanisms, is essential and should remain.

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 (European Commission). Focuses on ensuring transparency in economic transactions for minors, avoiding intermediate virtual currencies, and preventing exposure to in-app purchases on services presented as free.

Ensure transparency of economic transactions in an age-appropriate way and avoid the use of intermediate virtual currencies, such as tokens or coins, that can be exchanged with real money and then used to buy other virtual items, which can have the effect of reducing transparency of economic transactions and may be misleading for minors.

Feedback on the guidelines on protection of minors online under the Digital Services Act (The Safer Internet Centre Denmark (SIC DK)). Recommends default deactivation of donation and purchase functions for minors and calls for legislation to ensure greater transparency of virtual currencies beyond current platform-level measures.

Regarding the guideline described in line 653-657, we would like to add that the possibility for donating and making purchases on the platforms should be off by default for minors.

Contribution from medical professionals regarding the Draft Commission Guidelines on the Protection of Minors Online (Article 28 DSA) (Youth Smoking Prevention Foundation (Stichting Rookpreventie Jeugd); #vapenjouwkeuze). Urges expanding the regulatory focus beyond marketing to include platforms' role as marketplaces that facilitate potentially illegal or harmful commercial transactions directed at minors.

Expand the scope of "commercial practices" to hold platforms accountable for their role as de facto marketplaces.

Swedish Consumer Agency's comments on the draft 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 (DSA) (Swedish Consumer Agency). Contends that recommendations on virtual currency transparency and price practices should be handled under existing consumer protection law rather than through the DSA.

Hence, it is not appropriate that further recommendations are issued within the frames of the DSA.