The European Commission's Guidelines on Privacy, Safety, and Security for Minors under the DSA

Key takeaways

- The European Commission has published the final version of (non-binding) guidelines on measures to protect minors (U18) online
- The guidelines introduce stronger requirements for age assurance and verification, with the introduction of the EU age verification solution as a reference standard
- The guidelines expand obligations for default privacy and safety settings, including more granular controls
- The guidelines emphasize transparency, accessibility, and child participation, ensuring that minors and their guardians are informed and empowered
- The guidelines enhance moderation and reporting mechanisms, with a focus on rapid response, human oversight, and cross-platform cooperation

What are the key provisions and changes?	
Draft consultation guideline requirements	**Key changes to final guidelines**
Risk review	
• Requires providers to identify the likelihood of minors accessing the service, assess risks using the typology of risks (see Annex 1 of the guidelines), and consider the impact of measures on minors' rights.	• The frequency of the risk review has been expanded to require periodic (at least annual) reviews. • Adds new factors to consider, including metrics to monitor effectiveness, and requires the explicit participation of minors, guardians, and experts in the review process. • Stresses the need to publish outcomes (with appropriate safeguards) and to use existing children's rights impact assessment tools.
Age assurance	
• The guidelines describe three categories of age assurance: self-declaration, age estimation, and age verification. The Commission confirms that self-declaration is not considered to be an acceptable form of age assurance. • Age verification is considered by the Commission as an appropriate and proportionate measure to ensure a high level of privacy, safety, and security of minors in the following scenarios: (i) where products pose a high risk to minors, e.g., sale of alcohol, pornography, and gambling services; (ii) if a service's terms and conditions	• Material change. For scenario (iii) (see left-hand column for the draft proposal), the Commission has removed the qualification in relation to age verification for the risk identified to be "high," meaning that now **any** risk identified to minors' privacy, safety, or security relating to the listed categories of risk will require the use of age verification alongside access restrictions if those risks cannot be mitigated by other less intrusive measures as effectively as by access restrictions supported by age verification. • Age estimation can be used in addition to age verification techniques, or as a temporary alternative in the circumstances.

require users to be 18; (iii) where a platform has identified high risks to minors, including content, conduct, consumer and contact risks (e.g., arising from live chat, image/video sharing, anonymous messaging); or (iv) where there is a minimum age to access certain products of services offered and/or displayed on a platform. • Age estimation is considered appropriate in the following scenarios: (i) if a service's terms and conditions require users to be above a minimum age that is lower than 18; or (ii) if medium risk services are identified by the risk review.	
• Requires a proportionality assessment before implementing age assurance. Consider accuracy, robustness, reliability, non-intrusiveness, and non-discrimination. • Providers should offer more than one age assurance method and should provide redress for incorrect assessments.	• Introduces a requirement that online platform providers should make the result of an age assurance proportionality assessment publicly available. Stresses the need for robust, non-circumventable, and privacy-preserving solutions. • The Commission has added that age verification should be a separate process, not linked to other data collection, and should not allow storage of personal data beyond age group. • Platform providers should provide information about adequacy and the effectiveness of age assurance methods (e.g., by providing performance metrics).
• The EU age verification solution can facilitate age verification before the EU Digital Identity Wallets become available (expected by the end of 2026).	• The Commission has made an age-verification blueprint available. It currently only enables users to prove that they are over 18 when accessing restricted adult content, such as online pornography, but can be expanded to other age limits and use cases. • Clarifies that providers can use alternative age verification methods, but they must be compatible with the EU reference standard and meet the criteria set out in the guidelines. • Encourages providers to adopt "double-blind" age verification methods (i.e., methods to ensure that the platform does not receive additional means to identify the user and that the age verification provider does not know what the verification is for).
Account registration	
• This is one option to provide age assurance measures. • Registration processes should be accessible, explain benefits, and help users understand age requirements.	• The guidelines recommend carrying out age assurance where possible at the time of account creation. • Adds requirements for child-friendly language, ensuring that the registration process includes measures to help users understand if they are old enough to use the service, and avoidance of encouraging minors to share more information than necessary on their profile. • Emphasizes the need for easy account deletion and highlights the use of registration as an opportunity to inform users about safety features.
Default settings	
• Lists several specific examples where default settings are expected to be applied. • Default settings should be privacy- and safety-maximizing, with features such as private profiles, restricted contact, and disabled geolocation by default.	• None of the examples of default settings from the draft guidelines have been removed, but the list has been expanded, including adding that no one should be able to see the minor's activity such as likes or follows, and that recommendations of other accounts are turned off. • Expands the requirements for options to change settings (these should be presented in a neutral way and should be easy to return to default settings; warning signals should be presented when changing settings, explaining consequences). • Platforms should also consider whether it is necessary to go even further and implement more restrictive default settings and whether certain settings should be made irreversible or unchangeable for all minors or minors of a certain age (e.g., default settings for younger minors where no other user is allowed to engage in certain types of messaging interactions).

Online interface and design	
• Calls for child-friendly, accessible, and easy-to-use interfaces, and discourages persuasive design features that encourage overuse (e.g., infinite scrolling/rewards etc.). • Requires visible, customizable time management tools and positive nudges toward safer options that deter minors from spending more time on the platform.	• A new provision that AI features (e.g., chatbots) should not be automatically enabled for minors and that these must be risk-assessed before deployment. There should be age-appropriate transparency provided around the fact that AI interactions are different from human interactions and that AI can provide information that is factually inaccurate and can be misleading.
Recommender systems and search	
• Platforms should avoid reliance on extensive behavioral data in recommender systems and prioritize explicit user-provided signals, as well as empower minors to be more in control of their feeds. • Ensure that minors' search results and suggestions for contacts prioritizes accounts whose identity has been verified and whose contacts are connected to the minor's network or are contacts within the same age range.	• Enhanced recommendations around testing and adapting recommender systems.
Tools for guardians	
• Provides examples of managing screen time, setting spending limits, managing account settings, and seeing accounts the minor communicates with. • Gives appropriate transparency of the parental tools in place. • Providers should only allow changes with the same degree of authorization as required for initial activation.	• Emphasizes that platforms must never rely exclusively on tools for guardians. • Tools for guardians may also include features for managing default settings.
Commercial practices	
• Requires responsible marketing policies, clear labeling of advertising, and avoidance of exploitative practices.	• Requires pricing in national currency and tools for guardians to manage spending.
Moderation	
• Requires clear definitions of harmful content, moderation policies, and prioritization of moderation for content likely to harm minors.	• Adds requirements for 24/7 moderation, human review for high-risk content, moderation in all official languages of the member state, and specific channels for reporting fraud and suspicious financial transactions where a platform hosts such transactions. • Providers should explore the benefits of AI classifiers to help with moderation.
Reporting and user support	
• Requires effective, child-friendly reporting and complaint mechanisms, with prioritization of minors' reports. • Providers should confirm they have received reports, the process followed, indicative time frames, and possible outcomes.	• Introduces the need for support tools to connect minors directly to national helplines. • While reporting should be anonymous by default, there should be an option for minors to remove this (and, if so, it should be explained to minors when and how and what information is shared with others).

Governance	
• Providers should have a dedicated person or team and internal policies and procedures for ensuring compliance. • Terms and conditions must include certain information and should be searchable and easy to find. • Providers should adopt practices to assess the effectiveness of their measures, consult with minors and guardians, and make adjustments based on results. • Transparency should be child-friendly, age-appropriate, and accessible. Information should be provided to minors and, where relevant, guardians.	• Providers should consider making evaluations available for review and input by independent third parties (e.g., experts). • Information must be presented in the official language(s) of the member state in which the service is provided.