A&L Goodbody

TECHNOLOGY

Protection of minors on online platforms:

European Commission adopts Article 28(1) DSA Guidelines

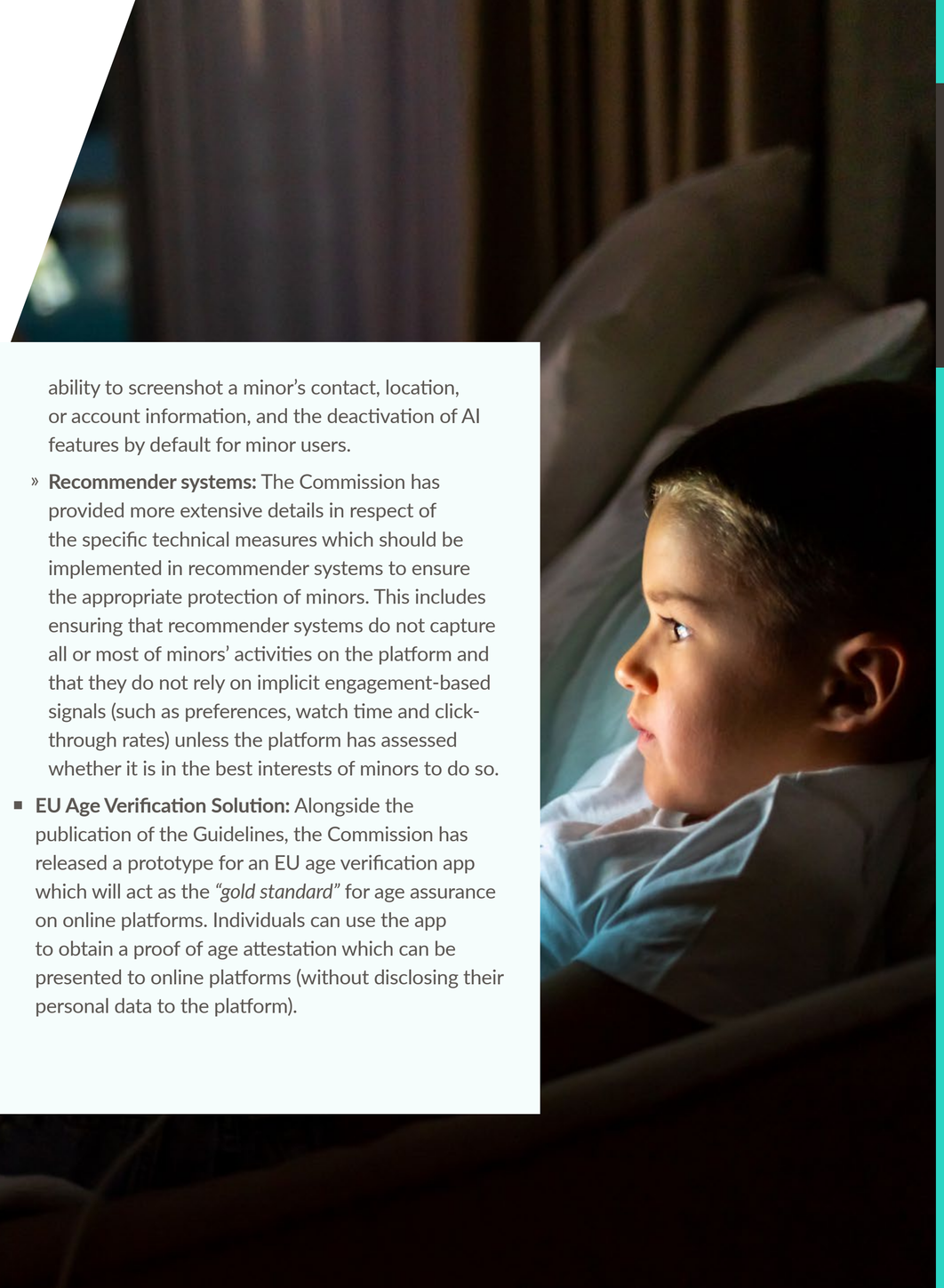
On 14 July 2025, the European Commission (the **Commission**) published its **finalised guidelines on the protection of minors** (the **Guidelines**) under the Digital Services Act (the **DSA**). The Guidelines were adopted following a public consultation on draft guidelines that were released in May 2025 (see **here** for our note on the draft guidelines).

In this article, we provide an overview of some of the key aspects of the Guidelines and highlight some of the notable changes which were introduced in the final version.

26 MIN READ

Key takeaways

- The intention is for the Guidelines to serve as a benchmark against which the Commission and Digital Services Coordinators (**DSCs**) will assess compliance with the Article 28(1) DSA obligation for online platforms providers to *"put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service"*.
- Article 28(1) DSA obligations apply to platforms which are *"accessible to minors"* and the Guidelines make clear that that concept should be interpreted broadly. In this respect, terms and conditions which prohibit a minor's use of the platform will not necessarily bring a platform out of scope of Article 28(1) DSA, if minors are, in fact, using the platform.
- The Guidelines set out a number of detailed expectations for online platforms accessible to children, including in respect of: (i) carrying out a risk review to determine the extent to which minors use the platform; (ii) implementing age assurance measures; (iii) default account settings; and (iv) the platform's content moderation and recommender systems.
- While many of the expectations from the draft guidelines remain in the finalised Guidelines, further detail has been added in a number of respects. In addition, there are a number of additional expectations which merit highlighting, including:
  - **Increased transparency obligations:** The final version of the Guidelines outlines the expectation that online platforms will make more information in respect of their safety measures publicly available. For example, platforms must publish (i) the risk review conducted in respect of risks to minors on its service; (ii) the assessments made regarding the appropriateness of age assurance measures; and (iii) performance metrics for those age assurance measures.
  - **Risk review enhancements:** The Guidelines now provide that the risk review must be conducted at least annually, when there are significant changes to the platform, or where there are circumstances around the platform's design or operation which impact the privacy, safety and security of minors.
  - **Account settings:** The Guidelines now call for new specific feature limitations such as restricting the ability to screenshot a minor's contact, location, or account information, and the deactivation of AI features by default for minor users.
  - **Recommender systems:** The Commission has provided more extensive details in respect of the specific technical measures which should be implemented in recommender systems to ensure the appropriate protection of minors. This includes ensuring that recommender systems do not capture all or most of minors' activities on the platform and that they do not rely on implicit engagement-based signals (such as preferences, watch time and click-through rates) unless the platform has assessed whether it is in the best interests of minors to do so.
- **EU Age Verification Solution:** Alongside the publication of the Guidelines, the Commission has released a prototype for an EU age verification app which will act as the *"gold standard"* for age assurance on online platforms. Individuals can use the app to obtain a proof of age attestation which can be presented to online platforms (without disclosing their personal data to the platform).



Purpose and status of the Guidelines

Article 28(1) DSA requires providers of online platforms which are *"accessible to minors"* to implement *"appropriate and proportionate measures to ensure a high level of privacy, safety and security of minors on their service"*. Article 28(4) empowers the Commission to issue guidelines to assist online platform providers in complying with that obligation.

The Guidelines are intended to serve as a *"significant and meaningful benchmark"* against which the Commission will assess compliance with Article 28(1). This implies a strong regulatory expectation that all online platforms which are *"accessible to minors"* (save for micro and small enterprises) will strive to align their practices with the Guidelines so as to meet their DSA obligations.

Scope of the Guidelines

When is an online platform "*accessible to minors*"?

The Guidelines make clear that an online platform provider cannot place itself outside of the scope of Article 28(1) DSA solely by including provisions in its terms of service that the service is not intended for use by individuals under a certain age.

The Guidelines reiterate the guidance provided in Recital 71 DSA, which notes that an online platform will be considered *"accessible to minors"* where any one of the following scenarios applies:

1. minors are permitted to use the service in the online platform's terms and conditions;
2. the service is directed at, or predominantly used by, minors; or
3. the provider is otherwise aware that *"some users"* are minors.

What exactly constitutes "some users" in the third scenario remains unclear, but the Guidelines do identify certain elements which will indicate that an online platform is *"accessible to minors"*, including:

i. the provider already processes personal data of those minors which reveals their age for other purposes;
ii. the online platform is known to appeal to minors;
iii. the online platform offers similar services to those used by minors;
iv. the online platform is promoted to minors; or
v. the online platform provider has conducted or commissioned research that identifies minors as users.

Accordingly, the Guidelines reflect the broad approach taken under the DSA (and other EU laws such as the GDPR and EU competition law), to focus any regulatory assessment on how the platform operates in fact, rather than merely assessing its intended use. If an online platform is not intended for use by minors, it will need to be able to demonstrate it has effective measures in place to avoid minors gaining access, otherwise it will be expected to comply with the obligations of Article 28.

Risk reviews

A notable development under the Guidelines is the expectation that online platforms accessible to minors should complete a risk review of their own services (and each time a significant change is made to its service) to determine the extent to which minors use the platform and, as relevant, the measures it has implemented to protect minors on its service.

Notable update to the Guidelines

The initial draft of the Guidelines outlined a number of elements which this risk assessment should cover, including:

i. the likelihood of minors accessing its service;

ii. the risks to privacy, safety and security of minors posed by the service by reference to the online platform's features such as design, marketing and uses[1];

iii. measures already taken by the provider regarding these risks;

iv. any additional measures identified in the review as appropriate and proportionate to ensure a high level of privacy safety and security for minors; and

v. the potential positive and negative effects on children's rights from any measures such as restrictions on children's rights to freedom of expression and information.

The final Guidelines added further details in respect of the elements which should be considered as part of the review, including:

- **Identification of metrics:** online platform providers must identify the metrics that it will use to monitor the effectiveness of any measures adopted to address risks to minors.
- **Categorisation of risks:** the risk review should contain an indication of the risk level to minors on the platform, e.g. low, medium or high risk, based on identifiable criteria.
- **Publication of risk review:** The draft guidelines provided that online platforms should *"consider"* publishing the outcomes of its risk review. The Guidelines now say that providers *"should"* publish the outcomes of the risk review (with appropriate redactions if necessary) and make it available to supervisory authorities.
- **Frequency of review:** After conducting an initial risk review, the draft guidelines outlined that further risk reviews should be conducted whenever a provider makes significant changes to their online platform. This provision has been enhanced to provide that the risk review should be performed:
  - at least once a year;
  - whenever significant changes have been made to a platform's design; and
  - where the provider becomes aware of circumstances that affect the platform's design and operation which are relevant for ensuring a high level of privacy, safety and security of minors.

The Guidelines note that, for the providers of very large online platforms and search engines (**VLOPSEs**), this *"protection of minors"* risk assessment can form part of the general assessment of systemic risks which is already required under Article 34 of DSA.

[1] *When considering what risks are posed to minors, online platform providers should consider the following types of risk: content, conduct, contact, consumer and cross-cutting risks (referred to in the Guidelines as "5C typology of risks").*

Age assurance methods

A central focus of the Guidelines is a discussion on age assurance measures. The Guidelines provide some further detail on what appropriate age assurance measures might look like under Article 28(1) DSA. However, they do not take a prescriptive approach in respect of what technical measures must be implemented. They instead discuss several potential measures which can be used in conjunction with one another, depending on the circumstances, and focus on the overall efficacy of the measures used.

Notable update to the Guidelines

The initial draft of the guidelines noted that, before deciding to implement access restrictions based on age assurance measures, online platforms which are accessible to minors should conduct an assessment of the appropriateness of those measures to ensure a high level of privacy, safety and security for minors. This provision is maintained in the final version but the final Guidelines also outline that platforms should make the result of that assessment publicly available, regardless of its outcome.

The Guidelines distinguish between *"age verification"* and *"age estimation"* measures and provide guidance in respect of the circumstances in which different types of measures may be most appropriate.

Age verification is defined in the Guidelines as a system that relies on physical identifiers or verified sources to confirm a user's age – e.g. a government ID. The Guidelines specifically identify four circumstances where access restrictions supported by age verification measures are considered appropriate. These are:

1. access to certain products or services which pose a high risk to minors and those risks cannot be mitigated by less restrictive measures e.g. the sale of alcohol or tobacco, granting access to any type of pornographic or gambling content;
2. the terms and conditions of the service require users to be adults; or
3. the risk review determines that the service is high risk.

Notable update to the Guidelines

The Guidelines introduce a fourth circumstance in which age verification is appropriate, namely where Union or national law prescribes a minimum age to access certain products or services offered on an online platform, including specifically defined categories of online social media services.

The inclusion of this additional category is notable as it has likely been included with an eye to ongoing discussions in a number of Member States[2] about introducing a mandatory age limit for the use of social media services. It is also noteworthy that the footnote to this new category specifically reminds Member States of their obligations to notify the Commission of any new draft technical regulations concerning information society services pursuant to the TRIS Directive 2015/1535. This reminder reflects the concern about how any such requirements would interact with the DSA, and the harmonisation sought to be achieved thereunder.

[2] *For example, in June 2025, French president Emmanuel Macron **said** he would push for a European Union regulation to ban social media for children under the age of 15, and if that cannot be achieved he would introduce the ban in France. France, Spain and Greece have been **lobbying for** the European Commission to introduce a social media ban for u15s, as have **Denmark**.*

Age estimation is defined in the Guidelines as a collection of methods which allow a provider to establish that a user is likely to be of a certain age, to fall within a certain age range, or to be over or under a certain age – e.g. facial age estimation. The Guidelines specifically identify two contexts where age estimation will be considered appropriate:

- where the terms and conditions of the online platform require a user to be above a required minimum age that is lower than 18 to access the service; and
- where the risk review determines that the service is medium risk i.e. not high enough to require age verification but not low enough to have no age assurance methods.

The Guidelines identify a list of general principles which should also be considered in assessing the appropriateness and proportionality of a proposed age assurance measure. These are:

- the accuracy and reliability of the measure;
- how easy it will be for minors to circumvent the measure;
- whether the age assurance method is intrusive and if another method would be less intrusive (and as effective); and
- whether the chosen method is non-discriminatory and accessible to all minors.

Despite this identification of specific instances where certain forms of age assurance methods should be used, the Guidelines also note that online platforms should generally offer users more than one age assurance method.

The Guidelines also explain, applying the above principles, that self-declaration should not be considered a sufficient age assurance measure. This is an unsurprising regulatory view and mirrors Coimisiún na Meán's position on age assurance, as set out in Sections 10.6(f) and 12.10 of its Online Safety Code. Equally, Ofcom do not consider self-declaration acceptable as a form of highly effective age assurance under the UK's online safety regime.

Notable update to the Guidelines

Transparency on age assurance: The finalised Guidelines include a new provision that providers must provide bespoke information about the age assurance measures they utilise, including information about how effective those measures are. As part of this provision, the Guidelines expect providers to outline performance metrics on age assurance measures, which include false positive and negative rates, accuracy levels and recall rates.

Personal data: The initial draft guidelines did not examine in detail the concerns raised by the European Data Protection Board (**EDPB**) in its statement on age assurance, namely that certain age assurance measures, while effective, may also necessitate the excessive collection of personal data from minors.

The finalised Guidelines do not go as far as to provide guidance on how to navigate this issue, but there is some further consideration of the issue. For example, the Guidelines encourage the use of anonymised age *"tokens"* which would constitute a suitable basis for providing age assurance without transmitting personal data. The planned EU Digital Identity Wallet (discussed below) would appear to facilitate this.

EU Digital Identity Wallet

The Guidelines discuss the forthcoming EU Digital Identity Wallet as a potential method of age assurance in the EU. The Guidelines provide some insight into how the EU Digital Identity Wallet will work – users will be able to use their digital wallet to only share specific information with online services, such as whether that person is over a specific age. Work in respect of the EU Digital Identity Wallet is ongoing and the Guidelines confirm that it is still scheduled for completion in 2026.

EU Age Verification Solution

Alongside the publication of the Guidelines, the Commission released a prototype for an EU age verification app (the **App**), which will act as the *"gold standard"* for age assurance online. Details on the prototype are available **here**. Individuals will be able to enroll on the App by a number of methods, including scanning an identity card/passport. They will then receive a Proof of Age attestation which can be presented to online services. The individual's identity and actions are said to be shielded from disclosure throughout the whole process.

The App now enters a pilot phase where it will be tested in collaboration with key stakeholders. Denmark, France, Greece, Italy and Spain are the first to pilot the App but market players (such as online platforms themselves) are also encouraged to take up the App and develop it further.

Account settings

An overarching principle of the Guidelines is *"privacy, safety, and security-by-design"*, meaning platforms accessible to minors should integrate the highest standards of privacy, safety and security for minors into the design and operation of their services. As an extension of this principle, the Guidelines expect default settings on minors' accounts to be configured in a manner that promotes privacy and security, while also discouraging excessive usage and harmful behaviour.

The initial draft of the guidelines set out a list of account settings which should be implemented as default on a minor's account. For example:

- **Limiting interactions:** accounts of minors should only allow interaction such as likes, tags, comments, direct messages or reposts by accounts they have previously accepted as *"friends"* or contacts. Furthermore, only accounts that the minor has previously accepted as contacts should be allowed to see their content and posts.
- **Limiting screenshots:** no account, except the minor's, should be able to download or take screenshots of content uploaded or shared by the minor to the platform.
- **Restriction of functions:** geolocation, microphone and camera, contact synchronisation as well as all optional tracking features should be turned off by default. The default autoplay of videos and hosting live streams should also be turned off.
- **Limitation of notifications:** push notifications should be turned off by default and should always be off during core sleep hours, adapting the core sleep hours to the age of the minor. When push notifications are actively enabled by the user, they should only notify the user about interactions arising from the user's direct contacts and content from accounts that the user actively follows or engages with.
- **Excessive use measures:** 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"*, should be turned off by default.
- **Body image measures:** filters that can have detrimental effects on body image, self-esteem and mental health should be turned off by default.
- **Availability of settings, features and functionalities:** As well as ensuring certain feature settings are installed as the default options on the accounts of minors, the Commission also notes that platform providers should consider if some settings or functionalities should be removed from minor accounts entirely and that irrespective of a minor's account settings, platforms should ensure that (i) minors can never easily be found or contacted by accounts they have not previously accepted; (ii) minors' personal contact details should not be disclosed to others unless the minor explicitly consents; (iii) minors should not be in contact suggestions to adult users; (iv) unknown users should not be able to view minors' activities (such as profile information, history, *"followers"*); and (v) minors should be able to restrict the visibility of certain content they upload.

Notable update to the Guidelines

The finalised Guidelines introduce the following additional recommendations:

- **Limiting screenshots:** This provision now outlines that no account whatsoever should be able to download or take screenshots of a minor's contact, location or account information in addition to the content they upload and share.
- **Restriction of activities:** No users should be allowed to view the minor's activities on the platform. This includes activities such as *"liking"* content or *"following"* another user.
- **No recommendations of accounts:** Recommendations for other accounts should be turned off by default.
- **Limiting tagging functionality:** Minors should be provided with the possibility to accept or reject any tagging by other users, whether in content, comments or otherwise.
- **Unwanted contacts:** Measures should be implemented to help prevent minors from inadvertently accepting unwanted contacts (e.g. by requiring users to include a message when trying to connect with a minor).
- **Restrictions on AI features:** AI features (such as chatbots and filters) should be deactivated by default for minors and they should not be *"nudged"* to use those features. AI features should only be available to minors after an assessment of the risks posed. These AI features should also not influence minors for commercial purposes.
- **Availability of settings, features and functionalities:** The finalised Guidelines proposed some additional account settings which platforms should implement for minors' accounts, irrespective of their chosen settings. These include the setting that minors should have the ability to accept or reject *"tagging"* in content or comments.

Commercial practices

Given the ability of unfair and exploitative commercial practices to negatively impact a minor's privacy, safety and security when using online platforms, the initial draft of the guidelines recommended that online platforms implement the following measures:

- **Appropriateness of advertising campaigns:** online platforms should consider whether certain advertising campaigns may not be appropriate for certain age groups.
- **Labelling:** while labelling commercial content will not be a new requirement for online platform providers, the draft guidelines stipulated that those labels should be accessible, child-friendly and consistent so that minors can easily recognise commercial content.
- ***"Disguised"* advertising:** minors should not be exposed to hidden advertising (and commercial content must be declared). This captures influencer marketing and product placements that may deceive minors into purchasing certain products or services.
- **Prohibition on exploitation:** minors should not be exploited by advertisers, influencer marketing and other commercial content – particularly where minors may lack commercial literacy.
- **Manipulative design techniques:** commercial content containing intermittent or random rewards, scarcity or persuasive design techniques that can lead to excessive or addictive behaviours should not be deployed on minors.

Notable update to the Guidelines

Further detail has been added to this section in respect of the measures which the Commission considers online platforms should adopt in order to guard against exploitative commercial practices, including:

- **Regular Reviews:** Platforms should regularly review protective measures relevant to commercial practices in consultation with minors, guardians and other stakeholders.
- **Volume of commercial content:** Platforms should ensure minors are not exposed to excessive volumes or frequency of commercial content, which could lead to excessive spending or addictive behaviours.
- **Restrictions on AI features:** Platform providers should not integrate AI systems into the platform that influence or nudge children for commercial purposes.
- **Transparency:** Platforms should ensure children are not exposed to techniques which reduce the transparency of economic transactions and which may be misleading for minors, such as a virtual currency that can be exchanged for real money and used to purchase virtual items. If minors are exposed to any in-app purchases, they should always be priced in the national currency.
- **Policy Reviews:** Platform providers should review their policies to offer economic transactions based on the evolving capacities of children, to ensure that certain age groups are not exposed to economic transactions where they do not understand spending and money.

Moderation

The initial version of the Guidelines outlined a number of measures that online platforms should implement to protect minors on their services. This included:

- **Harmful content and behaviour:** platforms should clearly and transparently define *"content and behaviour that is harmful for minors' privacy, safety and security"* within its terms and conditions, while ensuring that the fundamental rights of minors are not unduly restricted.
- **Enforcement of moderation policies:** moderation policies should include how harmful content and behaviour is moderated for minors including how it is detected and enforced in practice.
- **Moderation prioritisation:** platforms should *"prioritise"* moderation based on (i) the likelihood of the content causing harm to minors (ii) the impact of that harm and (iii) the number of minors that may be harmed by that content.
- **Technology and functionalities:** effective technologies, mechanisms and preventative features should be deployed by platforms to protect minors from harmful content or behaviour.
- **Restrictions on AI systems:** where an online platform offers AI systems, technical solutions should be adopted to prevent users from accessing, generating or disseminating content on or from that AI system that is harmful to minors. For generative AI systems, the initial draft suggested tools like prompt classifiers or filters to prevent minors being exposed to harmful content.

Notable update to the Guidelines

Further detail has been added regarding the measures which the Commission considers online platforms should adopt in respect of content moderation. The finalised Guidelines provide:

- **Human review:** The initial draft provided that platforms should *"consider"* human review in addition to automated review for content or accounts reported as harmful to minors. The Guidelines now provide that platforms must *"ensure"* human review.
- **Moderation teams:** Platform providers should have well trained and resourced moderation teams, with moderation mechanisms available 24/7. Providers should have at least one employee *"on call"* at all times for content moderation issues.
- **Moderation in all EU languages:** Content moderation systems and practices must be available in all EU languages the service is provided in.
- **Financial transactions content:** Where a platform accessible to minors hosts financial transactions, a specific reporting flow must be available for users (including minors) to report fraud and suspicious financial transactions.
- **Metrics:** The Guidelines state that online platforms accessible to minors should share their metrics on content moderation. This includes metrics on how often user reports are received, proactive detection rates, violation rates, the types of content reported and detected, and how the platform responded to those issues.

Recommender systems

The initial guidelines provided that recommender systems may result in risks to minors due to their ability to *"amplify"* content that can negatively impact their privacy, safety and security. The first draft suggested that platforms implement the following measures in respect of recommender systems:

- **Objectives of recommender systems:** platforms should consider parameters and metrics related to accuracy, diversity, inclusivity and fairness of minors when implementing recommender systems. This was said to contrast with typical metrics that platforms focus on such as optimising or maximising time spent by minors on the platform, or their engagement and interaction with the platform.
- **Behavioural data:** recommender systems should not rely on the ongoing collection of behavioural data capturing most of the minor's activities on the platform and should not rely on activity off the platform.
- **Contacts:** contact suggestions for minors should prioritise verified accounts, contacts "connected" to the minor's network and contacts in the minor's age range.
- **Signals:** platforms should prioritise explicit user-provided signals (user feedback and explicit preferences) over implicit engagement-based signals (browsing behaviour, watch time or click-through rates).
- **Harmful content:** platforms should prevent repeated exposure for minors of certain harmful content such as promoting unrealistic beauty standards, content that glorifies or trivialises mental health issues, discriminatory content, radicalisation content and distressing content.
- **Search features:** suggested terms and autocomplete functions should not recommend harmful or illegal content to minors. Platforms should block certain words or terms for minors that may trigger that content. If a minor searches for that content, platforms should redirect minors to appropriate resources and helplines.

The initial draft also outlined certain user control and empowerment measures in respect of recommender systems that should be available to minors. Those measures include:

- **Reset functionality:** minors should be able to permanently and completely reset their recommended feeds.
- **New content:** minors should be prompted to search for new content after a certain amount of interaction with a recommender system.
- **Profiling:** minors should be empowered to choose a recommender system that is not based on profiling.
- **Reporting and feedback:** platforms should ensure that their reporting and complaints mechanisms have a swift, direct and lasting impact on the parameters, editing and output of the recommender system. This can be achieved by removing reported content and contacts from recommended feeds and reducing the visibility of similar content.

The initial guidelines acknowledged that platforms are required under Article 27 of the DSA to disclose certain information in respect of recommender systems. The initial draft outlined that online platforms accessible to minors are expected to implement the following measures:

- **Transparency information:** minors should receive child-friendly and accessible information about why specific content is recommended to them and the parameters and users signals used for that recommendation.
- **Settings:** settings and information on recommender systems should be child-friendly and accessible.
- **Modifications:** minors should be able to modify or influence the parameters of their recommender systems by allowing them to select the types of content or activities they are interested in. These options should be available on account set-up and throughout the minor's use of the platform and should directly influence content recommended to the minor.

Notable update to the Guidelines

The finalised Guidelines outline the following additional expectations:

- **Risk review:** Recommender systems should be regularly tested and assessed as part of the risk review requirement outlined in the Guidelines (and discussed above).
- **Behavioural data:** If a recommender system relies on the processing of behavioural data about a minor, the suggestions of specific information made to minors should not rely on the processing of behavioural personal data that is so extensive as to capture all or most of the minor's activities on the platform.
- **Signals:** Recommender systems should rely on *"implicit engagement-based signals"* (preferences, time spent viewing content and click-through rates) only after the platform has assessed whether it is in the minors' best interests.
- **Profiling:** The initial draft outlined that platforms should give minors the option to choose a recommender system that is not based on profiling. The Guidelines now state that platforms should consider whether that option should instead be a default account setting for minors.
- **Child-friendly information:** The Guidelines has been updated to provide that minors should receive *"meaningful"* explanations about why certain content is recommended to them. Options related to recommender systems (such as options to modify the recommender system) should also have a child-friendly design and use child-friendly language.

User reporting, feedback and complaints

The initial draft of the Guidelines largely aligns with the final version in relation to user reporting, feedback and complaints mechanisms. This section supplements the obligations online platform providers are already required to comply with under Articles 16 to 18 and 20 to 22 of the DSA.

The Guidelines suggest that online platforms accessible to minors must ensure that their reporting, feedback and complaints mechanisms have the following features:

- **Content reporting:** users should be able to report content that is *"inappropriate"* or *"undesirable"* for minors or where minors may be *"uncomfortable with the idea"* of such content.
- **Underage accounts:** where online platforms have a minimum age requirement, users should be allowed to report suspected underage accounts.
- **Feedback:** minors should be allowed to provide feedback on content, activities, individuals, accounts or groups that they are uncomfortable with. This concept is quite subjective and the Guidelines note this can be achieved through allowing minors to select child-friendly options on content such as *"Show me less/more"*, *"Hide this"* or similar phrases.
- **Age assessment complaints:** where a platform uses age assurance methods, users should be allowed to lodge a complaint regarding the platform's assessment of their age.
- **Complaints mechanism:** the complaint handling mechanism that platforms must have under Article 20 of the DSA should contain certain *"child-friendly"* features. This includes ensuring that the mechanism (i) considers the fundamental rights of children, (ii) is intuitively and immediately accessible for minors (including those with disabilities or accessibility needs), (iii) is easy to use and understand and is age-appropriate, and (iv) is available to non-registered users if they can still access the platform's content.
- **Adapted mechanisms:** platforms should have a *"free text"* option in their reporting and complaints tools which allow minors to provide their own reasons for the report/complaint. If reporting categories are used, platforms should ensure that these are adapted to the youngest user on the platform.
- **Information sharing:** minors should have easy access to information about whether the platform discloses reports and/or complaints to other users. If that information is shared, minors should understand when, how and what information is shared.
- **Process information:** minors should be given information about the process that will be followed when reviewing their complaint and/or report, an indicative timeframe for making a decision and the possible outcomes.
- **Prioritisation:** reports and complaints submitted by minors should be prioritised and response times should be appropriate to the issue reported or complained.
- **Regular review:** platforms should regularly review reports, feedback and complaints to identify risks to minors and areas for improvement.

Notable update to the Guidelines

The finalised Guidelines introduce the following additional recommendations for reports, feedback and complaints:

- **Confidentiality and anonymity by default:** reports, feedback and complaints from minors should be confidential and anonymous by default. If a platform has to remove anonymity for minors, the reasons for this should be clearly explained.
- **Urgent reports:** platforms should give minors an option to indicate if the report is urgent, particularly in relation to ongoing privacy, safety, or security concerns.
- **Progress tracker:** it is suggested that platforms provide a mechanism for minors to track the progress of their report or complaint and allow them to communicate with platforms via that progress tracker.

User support measures

The initial draft of the guidelines recommended the following features to assist minor users in navigating platforms and seeking support:

- **Child friendly support:** user support measures should be clear, easily identifiable and accessible to minors. The support tools should directly connect minors to national support lines.
- **Warning messages:** if minors search for, upload, generate or share content that is illegal or harmful, or if a minor reports that type of content, a warning message should appear that links the user to national support lines.
- **AI support:** if platforms use AI features for user support, minors should be clearly warned that they are interacting with an AI system, that those interactions differ from human interactions and that AI systems can hallucinate and/or provide incorrect information.
- **Anonymous blocking or muting:** minors should be allowed to anonymously block or mute other users and/or accounts.
- **Comment restrictions:** minors should be allowed to restrict (and prevent) who can comment on their content and/or content about them.
- **Group functions:** minors should only be added to group functions where they are notified and have accepted an invitation to be part of that group.

Notable update to the Guidelines

The final Guidelines introduce the following additions to its user support recommendations:

- **Age-appropriate support:** the initial draft recommended that platforms link minors to *"national support lines"*. This has been updated in the final version, which now provides that platforms should link minors to the most appropriate support services for their location and age.
- **Limitations on AI:** the final version of the Guidelines has removed the section on AI support and now provides that platforms should limit AI support tools for minors, such that AI support tools should not be the main mechanism for interactions with minor users.

Tools for guardians

The Guidelines note that parental/guardian tools are *"complementary"* to child protection measures but should not be the sole measure used by platforms to protect children on its service (and it should not replace those measures). Parental/guardian tools should:

- Be easy to use, age appropriate and not disproportionate to minor's rights;
- Apply regardless of the device or operating system used to access the platform;
- Clearly notify minors that parental tools are activated;
- Only allow changes to the tools when authorised to the same degree required in initial activation; and
- Be compatible with the availability of interoperable one-stop-shop tools for guardians gathering all settings and tools.

Notable update to the Guidelines

- **Parental tools without an account:** The Guidelines add one important recommendation that guardians be able to use the relevant parental control tool without creating an account on the relevant service. There is no additional commentary around how this would be operationalised.

Governance

The Guidelines set out a number of expectations to ensure that protection of minors is prioritised and well managed by platforms. These governance expectations include:

- **Governance practices:** platforms should implement internal policies that aim to ensure a high level of privacy, safety and security for minors and appoint a dedicated person or team responsible for the protection of minors.
- **Designated person:** the dedicated person or team responsible for protection of minors should have direct access to senior management and should be a central point of contact for regulators, users and trusted flaggers in matters related to minors' privacy, safety and security.
- **Terms and conditions:** terms and conditions should be easily searchable and changes to terms and conditions should be logged and published. The Guidelines list information that should be included in terms and conditions, including information on how minors are protected on the platform and behaviour considered harmful to minors.
- **Monitoring:** elements of the platform concerning the privacy, safety and security of minors on the platform should be regularly monitored and evaluated. Platforms should regularly consult with stakeholders and civil society on child protection measures and the platform should consider adjusting the design and functioning of the service based on these consultations.
- **Transparency:** all information, warnings and communications to users recommended in the Guidelines should be presented to users in a child-friendly, engaging manner and should be easy to review.

Commentary

The measures envisaged by the Guidelines bring some further clarity as to what the regulatory expectations are likely to be around Article 28(1) DSA. Given the importance of protecting minors online, and the political environment around this issue, it is not surprising that the Commission has taken a broad view as to what could constitute a measure to ensure a high level of privacy, safety, and security of minors.

That said, a number of the suggested measures will have come as a surprise to non-VLOPSE online platforms, with the Commission's interpretation of Article 28(1) DSA in effect imposing a much higher degree of transparency and governance obligations than they may have expected. In particular, some non-VLOPSEs may consider that a number of the suggested measures are more akin to the types of obligations that the EU legislature had specifically reserved for application to VLOPSEs. In addition, both VLOPSEs and non-VLOPSEs may be surprised by the nature of some of the Commission's specific guidance on design and operational features.

Given that most popular platforms will likely fall within the scope of the Article 28(1) DSA, it now seems likely that a significant proportion of DSA enforcement will be assessed through the prism of Article 28(1) DSA and the Guidelines. In this way, Article 28(1) DSA has arguably been leveraged to substantially expand online platforms' substantive obligations under the DSA more generally.

That said, as proportionality will be a core principle in applying the Guidelines, it may be that providers can design less burdensome measures which achieve the same goals and are nonetheless acceptable to regulators as they prioritise the best interests of minors, and effectively safeguard their privacy, safety, and security.

What's next?

The Guidelines have now been adopted and may be used by DSCs as an interpretative aid when enforcing compliance with Article 28(1) of the DSA.

The Guidelines are subject to annual review and may be updated in the future to reflect practical experience, technological and societal changes, and other regulatory developments.

Notably, in respect of the age verification requirements specifically, the finalised Guideline state that even in contexts where age verification is appropriate (e.g. granting access to pornography or gambling content), age estimation measures may be appropriate as a temporary alternative for a limited, transitionary period not exceeding 12 months.

A&L Goodbody

Get in touch

If you would like any further information on the Commission's Article 28(1) DSA Guidelines, please contact one of the following or your usual contact on A&L Goodbody's Technology team.

Key contacts

Dr Stephen King
Partner
+353 1 649 2243
sking@algoodbody.com

Eoghan O'Keeffe
Knowledge Consultant
+353 1 649 2241
eogokeeffe@algoodbody.com

Jade Van Standen
Solicitor
+353 1 649 2780
jvanstanden@algoodbody.com

Resources

Commission publishes guidelines on the protection of minors — READ MORE

Protection of minors on online platforms – New EU Commission Draft Guidance on Article 28(1) DSA — READ MORE