Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.eu • @CCIAeurope

Europe

CCIA Europe's Feedback to Public Consultation

Guidelines for the protection of minors online under the Digital Services Act (DSA)

June 2025

The Computer & Communications Industry Association (CCIA Europe) welcomes the opportunity to contribute to the development of guidelines for the protection of minors, pursuant to Article 28 of the Digital Services Act (DSA). The Association believes these guidelines can help online platform providers ensure a high level of privacy, safety, and security for minors using their services.

In light of the recently published draft guidelines, and the European Commission's public consultation gathering stakeholder input, CCIA Europe offers the following feedback, structured around the main areas as referred to in the guidelines.

I. Structural improvements

As there is no effective one-size-fits-all approach to protecting minors, most online platforms opt for a combination of measures. It is therefore essential to ensure that the Commission's final guidelines under the DSA are appropriate, proportionate, and take into account the nature and specific characteristics of each service.

II. Risk review

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. The guidelines should prioritise general principles and standards for age-appropriate design of online services.

III. Service design

Online platforms vary significantly in their nature and unique characteristics. To ensure these guidelines are future-proof and remain adaptable to evolving trends, it is essential to adopt a flexible, proportionate, and predictable approach – one that builds on industry best practices and allows for meaningful adaptation across different services.

Introduction

The Computer & Communications Industry Association (CCIA Europe) and its Members are deeply committed to the protection of minors online. We firmly believe that children and young people should benefit from a high level of safety, security, and privacy in their online experiences. Article 28 of the Digital Services Act (DSA) is a fundamental piece of the puzzle in the broader effort to protect and support minors in the online space.

In today's global context, where the protection of minors is receiving increased attention, the draft guidelines presented by the European Commission are a welcome starting point. CCIA Europe appreciates that the Commission proposes a practical and harmonised approach in its minor-protection guidelines, supported by concrete examples and best practices.

However, we must emphasise that certain parts of the draft guidelines are heavily – if not overly – prescriptive and do not take into account the reality that there simply is no one-size-fits-all approach when it comes to protecting minors online. Indeed, in practice most online platforms opt for a tailored mix of measures to ensure that minors are safe and secure, that their interactions are private, and that they can access and use online services in a way that supports their growth, development, and freedom of expression.

This means that the measures specified in the guidelines need to be (more) proportionate and appropriate to each online platform's nature as well as the specific characteristics of the online services they provide. At present, there is still room for improvement in this regard.

To address this, the final guidelines should prioritise flexibility, predictability, and adaptability – focusing on the desired outcomes, rather than prescribing exactly how online services' features must be designed or implemented.

As the European Commission continues working to develop these guidelines to protect minors online pursuant to Article 28 of the DSA, CCIA Europe respectfully offers the following feedback in relation to some of the areas referred to in the guidelines:

    I.   Structural improvements
   II.   Risk review
 III.   Service design
         1. Age assurance
         2. Account settings, online interface design, and other tools
         3. Recommender systems

I. Structural improvements

As there is no effective one-size-fits-all approach to protecting minors, most online platforms opt for a combination of measures. It is therefore essential to ensure that the Commission's final guidelines under the DSA are appropriate, proportionate, and take into account the nature and specific characteristics of each service.

The Digital Services Act (DSA) rightly includes specific due diligence obligations and transparency requirements to ensure the safety and security of minors when using online services.

Since the DSA's entry into force, the Members of CCIA Europe have (even) further strengthened their efforts to ensure a high level of privacy, safety, and security for minors. In this context, we welcome the added clarity and practical examples provided by the draft guidelines, which should help online platforms in adequately adapting their services.

However, due consideration must also be given to the tools already implemented and considered by online platforms. This is currently not the case yet. Building on these existing tools would prevent the final guidelines from becoming overly prescriptive – which risks imposing highly burdensome, or even irrelevant, obligations on some online services, depending on their nature and primary audience.

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.

Rather than being overly prescriptive or technically detailed, the guidelines should focus on providing general principles and standards for age-appropriate design of services. They should establish a harmonised EU approach. The guidelines must prioritise providing clarity regarding the regulator's expectations and objectives over rigid or technical prescriptions.

The approaches taken by CCIA Europe's Members to protect children and youngsters online are continually evolving. All of them have dedicated teams focused on providing a safe and trustworthy experience for users, with particular attention for minors.

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. This requires a sufficient degree of flexibility. Such flexibility will help ensure that the guidelines truly serve as a future-proof tool – one that can be used as a blueprint for both existing platforms and new entrants seeking to develop or expand their services within the European market.

II. Risk review

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. The guidelines should prioritise general principles and standards for age-appropriate design of online services.

The draft guidelines establish an obligation for online platforms accessible to minors to carry out a risk review whenever they make significant changes to their services. They also include a recommendation to consider publishing the outcomes of such reviews. CCIA Europe welcomes the effort to streamline the risk-review process, particularly through alignment of the draft guidelines with the risk assessment requirements set out in article 34 of the DSA for providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs).

Computer & Communications
Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.eu • @CCIAeurope

Europe

Yet, more should be done to further align the draft guidelines with platforms' existing risk assessment mechanisms. For example, as noted above, the draft guidelines state that providers should carry out a review whenever they make any "significant change to their online platform." By contrast, the current risk assessment framework under Article 34(1) of the DSA requires such assessments only "prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article."

Moreover, the Commission's draft suggests that complying with the guidelines – either partially or in full – may not be enough to meet the obligations for VLOPs and VLOSEs under Articles 34 and 35 of the DSA. Given the detailed and extensive list of best practices outlined in the draft guidelines, it remains unclear what "additional measures" may still be required from VLOPs and VLOSEs in practice.

For online platforms that are not classified as VLOPs or VLOSEs under the DSA, the same level of granularity in risk-review requirements may not be appropriate. Right now, the draft guidelines fail to account for the fact that certain online platforms may not have the resources to carry out a risk review each time their services are modified.

The guidelines also impose several obligations on all online platforms, irrespective of the outcome of the risk assessment. For instance, the obligation to analyse the number of users and uses (actual and expected) or the potential positive and negative effects on children's rights of any measure that the provider currently has in place. CCIA Europe believes that a more proportionate approach would target the application of best practices to those platforms that are genuinely likely to be accessed by minors – and only where such access is likely to pose a material risk to the minors.

The suggestion to publish the outcomes of the risk review should be approached with more caution. While transparency may have certain benefits, it must be carefully balanced against the need to protect personal data and confidential commercial information. Perhaps even more important, the guidelines should also recognise that the risk reviews may contain sensitive data points or other information that could be exploited by actors with malicious intent when published. For this reason, strict adherence to data protection principles is essential to guarantee the confidentiality of such reviews and to avoid undermining the very protections for minors they aim to support.[1]

CCIA Europe believes that any requirements introduced in the final guidelines should avoid unnecessary duplication of existing risk-assessment processes already in place. The guidelines should allow for diverging methodologies when assessing risks – beyond the 5Cs typology of risks – provided that these assessments are transparent, shared with competent authorities, and proportionate to the identified risks.

III. Service design

Online platforms vary significantly in their nature and unique characteristics. To ensure these guidelines are future-proof and remain adaptable to evolving trends, it is essential to adopt a

---

[1] Further details on CCIA Europe's views as regards access to data can be found in CCIA Europe's feedback on the European Commission's draft delegated act on data access for researchers (December 2024), available here.

flexible, proportionate, and predictable approach – one that builds on existing industry best practices and allows for meaningful adaptation across different services.

1. Age assurance

As recognised by the Commission in the draft guidelines, a variety of approaches to age assurance exist. The most common fall into the categories of self-declaration, age estimation, and age verification. Age assurance is a complex issue with no universal solution that can be applied across the board.[2] Each approach presents unique trade-offs in terms of accuracy, liability, privacy, and security.

That is exactly why online services often combine different methods, depending on factors such as the type of service, target audience, perceived risks, users' privacy and security expectations, or economic feasibility, to name just a few.

Age assurance requires careful balancing of multiple factors – including security, privacy, and data collection. Hence, CCIA Europe welcomes the draft guidelines' recognition that a spectrum of age-assurance methods exist, and that no online service is like another. We particularly appreciate the Commission's efforts towards fostering a unified and harmonised approach.

Nevertheless, CCIA Europe emphasises that while age assurance could play a valuable role in creating a safer online experience for minors, it should never serve as a standalone solution, an isolated policy choice, nor as a goal in itself. Age assurance should always be viewed as one element within a broader strategy to mitigate risks and support age-appropriate design of online services.

Measures aiming to introduce age assurance should be proportionate to the risk profiles of the different online services and flexible, making sure that those services posing the highest risks for minors are held to the highest standards. In other words, a one-size-fits-all solution would be inappropriate for the diverse digital ecosystem.

Indeed, the draft guidelines should explicitly acknowledge the value and effectiveness of combining various age-assurance methods, including self-declaration and age estimation. Particularly for those services that present a low risk, the guidelines should not solely focus on verification relying on physical identifiers – as this would be intrusive and disproportionate. The guidelines should also better explore ways in which the overall ecosystem can collectively bring about effective means of child safety and age assurance online.

The draft guidelines suggest that age verification is appropriate when certain products or services have a minimum-age prescription, such as the sale of alcohol. 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.

---

[2] The Digital Trust & Safety Partnership (DTSP) has developed a comprehensive overview of the guiding principles and best practices on age assurance. These can be found here.

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. 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 limitation.

In parallel to the development of these guidelines, the Commission is carrying out important work on an age-verification solution that is compliant with the European Digital Identity Framework (eIDAS Regulation).[4] Nevertheless, it is too early to consider this as a mature option. Its effectiveness, reliability, and user adoption remain untested. Since only VLOPs would be required to accept the 'digital wallet', it is unclear how such a system would contribute to improving safety, privacy, and security across the whole ecosystem.

CCIA Europe advocates for transitional solutions that adequately balance safety and privacy, while guaranteeing a harmonised EU-wide approach. 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.

To ensure broad adoption and build user trust, any age-verification framework must be harmonised and standardised, as well as predictable, effective, user-friendly, easy to adopt, interoperable, and scalable.[5]

2. Account settings, online interface design, and other tools

On parental control systems, 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. Such a framework should also support innovation and interoperability. The parental controls proposed in the draft guidelines, however, must allow greater flexibility in implementation.

Overly prescriptive requirements mandating certain platform-design features by default may unintentionally alter user behaviour and restrict minors' ability to make informed choices. CCIA Europe recommends developing technical standards grounded in industry best practices that enable the adoption of an EU-wide interoperable framework.

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. This approach also fails to take into account the different context faced by each platform, as well as the fact that both technologies and associated risks continue to evolve over time. For example, there are a

---

[3] Regulation (EU) 2016/670 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available here.
[4] Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, available here.
[5] Further details on CCIA Europe's views on age assurance can be found in CCIA Europe's Recommendations on Age Assurance (February 2025), available here.

![CCIA Computer & Communications Industry Association — Open Markets. Open Systems. Open Networks.]

ccianet.eu • @CCIAeurope

Europe

number of parental-control notifications that may include important information in terms of security, safety, or other account-related features.

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. Prescriptive default settings or added friction (i.e. specifically designed to deter users from certain actions) would also risk being considered as "dark patterns" as defined in Recital 67 of the DSA.

Moreover, there is a growing concern that minors may develop 'click fatigue' if constantly prompted to opt in or out of settings or make repeated choices before being allowed to post or view more content. Such an approach would hinder the ability of children to enjoy an online experience that enhances their creativity and socially enriches them.

Finally, the objectives behind certain measures prescribed by the draft guidelines remain unclear. CCIA Europe recommends that the guidelines clearly define their intended expectations and prioritise outcomes, rather than focus on prescribing specific solutions. It may very well be that a combination of measures or alternative options can achieve the same desired result.

3. Recommender systems

Recommender systems provide significant value and allow minors to discover high-quality and relevant content that is appropriate for their age. Maintaining personalisation is crucial for online platforms to continue delivering this experience. CCIA Europe welcomes the guidelines' recognition of the importance of recommender systems but encourages further clarity on this point.[6]

These systems differ widely across platforms, also based on the risk level of the recommendations provided. The measures in section 6.5 of the draft should be targeted, instead of universally applying to all online platforms. For instance, the draft guidelines now suggest introducing a "reset" option for a provider's recommender system, when this could severely impact the user experience, without any guarantees that it provides safety benefits for the vast majority of users.

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.

There is a very delicate balance to be struck between empowering minors to control the features of the online services they use and allowing platforms to help them discover tailored enriching and age-appropriate content. This requires effective controls and moderation techniques to be combined.

CCIA Europe believes that the final guidelines on minor protection should acknowledge that use of certain behavioral data – used with the utmost respect for personal data protection –

---

[6] Further background on online personalisation can be found in CCIA Europe's Explainer on Understanding Online Personalisation (October 2024), available here.

Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.eu • @CCIAeurope

Europe

can support the delivery of personalised content that is beneficial, educational, and age-appropriate for minors.

Personalised recommendations can also help reduce repeated exposure to certain content that, while harmless when viewed once, may become problematic with excessive viewing. Recognising the diverse developmental stages and evolving judgement of minors is crucial to ensuring that protection measures also match their expectations when accessing and consuming content online.

Conclusion

The safety and well-being of minors online is a shared responsibility that requires a whole-of-society approach. While the Commission's draft guidelines are a valuable starting point, further refinements are needed to ensure the resulting framework is truly appropriate and proportionate. Only then can these guidelines serve as a future-proof reference for online platforms striving to meet EU standards for minor safety, security, and data protection.

Designing the right policy framework means striking a careful balance: one that safeguards the rights to safety, privacy, and security, while also preserving the many benefits that digital services offer for minors' learning, development, and self-expression. This is a complex challenge, but an essential one.

CCIA Europe and its Members remain deeply committed to actively promoting safety, trust, and inclusivity across the digital ecosystem, particularly for younger users. Continued collaboration among all actors is essential, alongside strong commitment to high standards of protection and meaningful empowerment for minors in their online experiences.

Together with its membership, the Association looks forward to continuing its constructive engagement with the European Commission to help ensure that minors are effectively protected online, that the implementation of the overall DSA remains consistent across the EU, and that legal certainty is upheld for both users and businesses.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policymaking since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policymaking in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:
CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org