DOT europe
Digital • Online • Tech

November 2023

DOT Europe position

Code of conduct on age-appropriate design under the Better Internet for kids strategy (BIK+)

DOT Europe welcomes the opportunity to participate in discussions regarding the proposed age-appropriate design (AAD) code foreseen under the new European strategy for a better internet for kids (BIK+)[1], published in May 2022. Following up from the initial meeting of the expert group, we would like to propose a way forward to ensure a targeted and achievable approach that facilitates the delivery of a concrete outcome in time for Safer Internet Day 2025 as proposed by the European Commission.

Indeed, it was suggested during the first meeting of the Special group, that the Code should reflect the three key words of Article 28(1) of the Digital Services Act (DSA): privacy, safety and security. Age assurance is also an important issue to tackle in the BIK+ Code. Our paper thus puts forward a set of principles that we believe will inform the European Commission in the development of a proportionate, risk-based, and future-proof code.

Given Member States and industry stakeholders are keen to achieve a EU AAD Code as promptly as possible, with some pushing for a solution even before the proposed time frame of February 2025, we would propose a phased approach to the work on the AAD Code. This would allow the group to focus on delivering on one of these aspects first, in time to meet the European Commission's 2025 deadline. This approach would allow for a more in-depth examination of the rest of the issues at a later stage and still in the framework of the Code.

Given the ongoing discussions on the proposal for a Regulation laying down rules to prevent and combat child sexual abuse and the recent entry into force of the DSA, as well as the European Commission's ambition, we would recommend to focus first on two key areas so that we have concrete achievable outcomes to work towards. The two areas we suggest to focus on are (1) safety issues, which is a topic aligned with the current legislative focus on online safety; and (2) a pragmatic and harmonised process on age assurance based on the urgency to tackle this issue.

A risk-based approach to working on safety

The intention is to develop a Code that could apply to different products and services, with a shared goal of protecting children across the relevant technical landscape. We thus recommend putting forward a **risk-based, systems approach**.

[1] A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN

Such an approach is necessary because several aspects come into play when it comes to how children use online services and this will help ensure that the code address the variety of the relevant parts of the current ecosystem:

- **Recognising developmental stages within the children group:** Different age ranges (e.g. under 13 years old, from 13 to 15 years old, from 15 to 17 years old) present fundamentally different risk profiles, as well as varying degrees of autonomy and different developmental stages. For example, while parental controls may work for children, an approach that is more geared towards supervision and guidance would be appropriate for teenagers, who are more autonomous.
- **Modular approach to commitments:** Relevant online services used by children are varied, both in terms of service type and in terms of the age profile of users. Although comprehensive, the Code should allow enough flexibility for relevant service providers to choose the most appropriate commitments based on their level of risk and relevance to their services. This also means that the Code should refrain from mandating specific product design solutions or integrations to avoid unintentionally diminishing the variety of services on offer. This approach also means that any commitments will be future-proof.
- **Proportionality:** Commitments under this Code should be proportionate to an identified risk and purpose of a product on the signatory's service. Relevant services or products should be identified for inclusion based on known risks to children. Different products coexist on a single service and they each require a different solution to ensure age appropriateness (e.g., in certain cases the exact age of the user is needed, in other cases a broad range would suffice, in other cases it is not necessary at all).

To follow a risk-based approach, in addition to bearing the three principles above in mind when discussing commitments, we recommend integrating the risk assessments conducted by providers pursuant to the DSA for their relevant services as it would build on existing and available evaluation. The risk level of a relevant service would then be corroborated and backed by the DSA risk assessment which would be an established process.

It should be noted that some services should not be covered by the scope of the Code because they will not be relevant and/or cannot deliver the objectives.

Finally, DOT Europe stresses the need for the Code to **encourage, not mandate** the design of campaigns, tools or features to protect young users' wellbeing while using signatories' products so as to allow for better tailoring and adaptation of the solutions.

A much needed focus on age assurance

Different measures deployed by in-scope service providers contribute to ensuring an age-appropriate design and a safer online experience for children[2]. These include *inter alia* communications to users, default settings, parental control tools, as well as age assurance. However, should the Commission be

[2] Some of the current practices are listed in our position paper on the proposal for a Regulation laying down rules to prevent and combat Child Sexual Abuse, available at https://doteurope.eu/wp-content/uploads/2022/12/DOTEurope_PP_CSAReg_Compilation-1.pdf

willing to deliver the first results of the Code soon, we recommend a focus on age assurance that would take the recommendations outlined in this paper into consideration.

Definitions

As a matter of clarity, we recall that age assurance covers declared age, age verification and age estimation techniques. Whereas age verification is based on evidence that someone is above a certain age or is part of a certain age range, age estimation typically relies on artificial intelligence which, for instance, uses users' behaviour on the service to determine their age range[3]. In this paper, we use 'age assurance' in order to encompass different methods used by service providers and to underline that relevant parts of the service that are accessible to children may not all need the same age assurance method because of their different risk levels.

DOT Europe urges the Special Group to address the issue of age assurance as a priority and take the industry's feedback into account. We suggest this due to the fact that a multistakeholder engagement will be necessary to find proportionate and effective rules in view of the current debate on safety for children and adults and of the obvious emergence of national initiatives attempting to tackle this issue.

Avoid the fragmentation of the Single Market

Some Member States are introducing varied age assurance frameworks. While we welcome the work to ensure greater safety online, we believe that, in order to maintain the integrity of the Single Market, it is crucial that a framework is agreed at EU level. Indeed, the cross-border nature of the services would make it challenging for providers of in-scope services to implement different requirements in each Member States. Furthermore, existing EU law should serve as the basis for an EU action on age assurance.

The French law n°2023-566 "visant à instaurer une majorité numérique et à lutter contre la haine en ligne"[4] is a prime example of a single initiative which could disrupt the harmonisation sought by the DSA, as an horizontal legislative framework which paves the way for an EU action on age assurance. In Germany, the Committee for the protection of minors in the media ("Komission für Jugendmedienschutz") has also developed its own evaluation procedure of age verification systems[5]. A number of other activities in the field of age assurance are currently being discussed at international level: the UK Online Safety Act, the American Protecting Kids on Social Media Act, CEN-CENELEC workshop agreement on age-appropriate digital services network or the start of an ISO standard on age assurance systems[6]. In order to avoid differing requirements for providers in different smaller jurisdictions, we see high value in agreeing at EU level on a common framework for age assurance.

[3] An helpful taxonomy is available in the paper published by the Digital Trust and Safety Partnership, available here: https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf andon the Age Verification Providers Association's website: https://avpassociation.com/definitions/

[4] More information on this law can be found here: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047256856/

[5] More information can be found here: https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme/

[6] Since then deleted: https://www.iso.org/standard/80399.html

Building on the existing environment for age assurance

If we agree that an action at EU level is necessary to avoid competing frameworks on this topic, then it is also necessary to acknowledge that the Code needs to fit, build on and complement the existing EU legislative framework.

Many of our members have already put in place measures aimed at providing a safe online experience for children on their services. We would thus recommend for the Code to **build on current best practices** implemented by in-scope service providers to protect their respective child users and remains proportionate to the risk identified and the type of service concerned, in order to facilitate implementation.

In addition to acknowledging what is currently in place, it is crucial that the Code complements relevant pieces of the current legislative framework and not overlap it. The BIK+ strategy rightly mentions the Digital Services Act and the Artificial Intelligence Act but DOT Europe underlines that there is a broader legislative framework in place already, notably in relation to data protection. We therefore welcome the mention of AVMSD and GDPR in the terms of reference since the Code should build upon a comprehensive legislative framework pertaining to all relevant child safety issues identified previously. It should furthermore adopt the approach of some of the cornerstone legislation developed, e.g. the principles of the GDPR, tech neutrality and a risk-based approach to ensure consistency and achieve a future-proof framework. The European Commission itself has been working on frameworks for age assurance, both legislative (eID Regulation) and non-legislative (the euCONSENT project, funded through a European Commission grant).

Further to ensuring that the BIK+ Code fits into the existing legislative and non-legislative environment, this Code is an opportunity to foster harmonisation between relevant service providers to ensure a smooth user experience.

Our recommendations for an age assurance framework under the BIK+ Code

In view of the focus of the BIK+ Code on age assurance, we respectfully share several recommendations for the Special Group. Several organisations have already published interesting suggestions for an age assurance framework[7], which are reflected to some extent below.

Any discussion on an age assurance mechanism should take the following principles into account:

- **Balanced risk-based approach**
    - Appropriateness to the identified risk level of a service.
    - The necessary level of assurance should change depending on the portion of the service that a user is trying to access and related risks.

[7] For instance, DTSP paper mentioned above, or the Center for Information Policy Leadership shared takeaways from their age assurance roundtable, held in February 2023: https://www.informationpolicycentre.com/cipl-blog/age-assurance-and-age-verification-tools-takeaways-from-cipl-roundtable

    - The positive and negative impacts of the service on fundamental rights[8] and children's rights[9] should be considered when evaluating the risk level of a service.
    - The method implemented must also be proportional to the risk of getting it wrong, i.e. consider the impact for both undetected teens and miscategorized adults.
- **Preserving privacy and protecting data**
    - It is crucial that we minimise the additional data being collected to verify age. Any recommendations to providers of in-scope services on age verification and assurance to protect children would need to be in full respect of EU privacy and data protection rules. Although we recommend applying a risk-based approach to the use of age assurance mechanisms, all users' privacy should be preserved when accessing some parts of relevant services. We would thus welcome the involvement of the EDPB on any relevant discussions and would call for guiding documentation in order to help providers meet expectations of the BIK+ Code.
- **Effectiveness and accuracy**
    - Age assurance should generate reliable results and be built on systems that are designed to be difficult to circumvent, to allow services to provide users with age-appropriate experiences.
- **Accessibility and inclusiveness**
    - Age assurance methods should be bias-free, including when it comes to facial recognition. Additionally, users who do not possess identification documentation, which is often the case for minors, should still be able to use the service so as not to exclude them from online experiences.
    - Another parameter to bear in mind is users' preferences. They should have the choice between different age assurance methods as some are comfortable with e.g. facial estimation, others with identification based on official documents.
    - Meaningful user transparency and appeals tools must also be accessible for a wide range of users (e.g. age, background).
    - We strongly recommend the consideration of children's experiences and perspectives on any proposed age assurance solution, and of their interests and rights to be in the context of data protection discussions – while children are entitled to privacy, they also have a right to freedom of expression and to autonomy that online communities provide.
- **Affordability**
    - Since the BIK+ Code aims at reaching a wide variety of services, in terms of service offering and size, the framework developed in the Special Group should remain focused and affordable for smaller service providers willing to ensure safer online experiences for their younger users.
- **Interoperability**
    - In order to maximise the uptake of the age assurance framework, the European Commission should encourage interoperable solutions so users will be able to enjoy a smoother online experience.
    - To ensure proportionality of the mechanism, we note however that it would be important to define who exactly bears the responsibility to put in place age assurance

[8] See in particular the EU Charter of Fundamental Rights and the European Convention on Human Rights.

[9] See in particular the UN Convention on the Rights of the Child.

methods. It should however be the responsibility of the service provider to establish how age determines child access to all or part of their services.

To conclude, the Code needs to strike a fair balance between different interests, e.g., protection of personal data, child protection, child digital empowerment, self-determination and accessibility. We furthermore underline that industry should be given an active role in building these standards.

Concluding remarks

We strongly encourage the Commission to consider these recommendations when deciding on a path forward for the BIK+ Code to enhance the safety of children online. In addition to the industry views expressed in this paper, we also point to the need to base the Special Group's work on actual research and scientific evidence regarding e.g. children's developmental stages, the different methods of age assurance to ensure the BIK+ Code remains relevant and accurate.

This initiative is an excellent opportunity to reach a common framework around child safety online and age assurance mechanisms. DOT Europe hopes a constructive and pragmatic dialogue will start very soon on these topics to make sure the Special Group completes the first stage by 2025, bearing in mind that many members of the Special Group will need to consult with their members before agreeing on any proposed positions.

Annex: DOT Europe principles for a BIK+ Code

1. The scope, desired outcomes, purpose and guidance for the Code should be clear from the outset as regards the timelines envisaged and the aims of the Code. A viable amount of time should be allocated to the drafting process and to the implementation period for the process to be fair on all stakeholders involved.
2. The Code should be proportionate and identify products/services that are high risk to children.
3. The drafting process should gather all relevant parties, from children and parents to all relevant service providers, including device manufacturers and mobile operators). The Code's design should be a multi-stakeholder, consensus-led effort: safety, privacy, child protection, child digital empowerment, self-determination, accessibility and child development experts should be part of the discussion and the objective should be to develop common standards to achieve outcomes that a diverse group can agree on and defend.
4. The Code should take a risk-based, systems approach. For age verification, commitments should aim at proportionate systems that consider the cost of getting it wrong and potential impact to both undetected teens and misclassified adults.
5. The Code should be flexible (in terms of measures the companies can implement and in terms of entities covered) in order not to stifle innovation, e.g. parental controls are a viable tool (as part of a wider toolbox), as long as they respect teens' privacy and their developing autonomy. Those controls should amount to supervision and/or guidance, not consent, and they should remain optional.
6. The Code should allow for sufficient flexibility to apply to different products and stand the test of time. It should not mandate specific product design solutions or integrations.
7. No single age assurance method or age verification tool should be mandated. Instead, signatories should be encouraged to offer a variety of accessible tools, with sufficiently reliable results, that require a minimum amount of additional data collection proportionate to the risk.
8. The Code should encourage the design of campaigns, tools or features to protect young users' wellbeing while using signatories' products.
9. The Code should build upon existing legislative framework and adopt the approach thereof (e.g. principles of the GDPR, tech neutrality…).