Federal Agency
for Child and Youth
Protection in the Media

KidD.bund.de
Federal Office for the Enforcement
of Children's Rights in Digital Services

Comments on the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065

The Federal Office for the Enforcement of Children's Rights in Digital Services (KidD) and the Federal Agency for Child and Youth Protection in the Media (BzKJ) welcome the first public draft of the guidelines as an important approach for the protection for children and young people on a broad level.

Many of the proposed measures are consistent with our previous practices, as well as with insights gained in other work processes, such as the work of our Advisory Board and the dialogue and engagement format *ZUKUNFTSWERKSTATT* of the BzKJ.

KidD sees the necessity of several amendments and clarifications to optimize the guidelines to guarantee a safe usage of online platforms for minors.

General Remarks

I. The protection of the personal integrity of minors

Protecting the personal integrity of minors is a key obligation for all stakeholders involved in modern child and youth protection in the media. Particularly concerning interaction risks, safeguarding personal integrity is essential for adequate media protection.

An explicit reference to the significance of the protected interest of personal integrity should be included to clarify the definition of the scope of protection within the framework of the objective description of Article 28(1) DSA.

II. Need for flexibility regarding national law enforcement

It is essential that the Commission continuously reviews the guidelines and adjusts as necessary. The work of Working Group 6 should be maintained to guarantee ongoing exchange of experiences and best practices of possible amendments.

The working group should also include experts and stakeholders on specific topics. The organisation *jugendschutz.net*, for example, has exceptionally high levels of expertise in the area of necessary precautions and risks in Germany.

At the same time, it is necessary to emphasize the responsibility of national law enforcement authorities more clearly. They should assess, on a case-by-case basis, whether the measures

have been properly implemented and should also be able to determine which protective measures should be taken in each individual case – even cumulatively. This clarification and encouragement of national law enforcement are crucial to fostering innovation and flexibility in addressing additional requirements in specific cases.

Future revisions of the guidelines should be carried out in close cooperation with the national supervisory authorities, as well as with the involvement of other experts.

III. Greater consideration of AI

The guidelines provide important guidance in several areas, including the Commission's assessment of AI usage, the measures that can enhance protection, and the relevant risks posed by AI. It is equally important to recognize the opportunities AI creates: particularly in the protection of minors, AI can assist in detecting inappropriate (sexual) advances and content. AI has become an integral part of everyday digital life; this aspect should be given even greater emphasis within the guidelines.

KidD recommends including the following aspects:

- All implemented AI should be disclosed, and the mechanisms made as transparent as possible, particularly chatbots integrated into the services, along with their potential uses and functionality. All implemented elements also fundamentally serve security purposes. At the same time, AI should be able to be switched off and reset as far as possible.

- The datasets and programming should offer the highest level of security and – depending on the platform's focus – be sensitive to typical problems faced by children and young people.

- AI – esp. AI Chatbots – should also provide easily accessible internal support as well as platform-independent, low-threshold external assistance. Furthermore, child-friendly help areas should be made available on the platforms in an accessible and user-friendly manner.

- Chatbots should under no circumstances exacerbate problems and crises among minors by, for example, dangerous behavior, encouraging self-harming or triggering behavior, etc. Autocomplete should result in age appropriate content.

- Furthermore, there should be a mandatory labeling requirement not only for dedicated AI platform elements but also for users wishing to contribute AI generated content (including AI accounts) to the platform. In such cases, labeling should be mandatory and made available to users when content is uploaded.

- The „state of the art“ in AI is not easily transparent to online platform operators. Given the rapidly evolving nature of this technology, substantial education and guidance are required. It would be desirable for the Commission to periodically summarize the essential state of the art in an easily understandable manner. This process should involve collaboration with experts from academia, civil society, stakeholders, and other members of the responsible community to provide regular updates on current developments.

Specific Comments (based on the structure of the guidelines)

I. Scope

The scope of application of Article 28(1) DSA should be as broad as possible. In this respect, the clarification that a mere reference to the terms of use, “e. g., from 18,” is insufficient to exclude the platform from the scope if it remains accessible to minors is very welcomed.

The exact delimitation between the principal service and minor functionalities is still in need of clarification. This issue is particularly relevant for online games, where the role of communication functions — whether principal service or minor functionality — must be clarified when the main focus is on gameplay. In this regard, the guidelines could provide important details to further differentiate typical functionality in the context of minor users, thereby offering providers valuable guidance.

II. Risk Review

The risk review is an important tool for raising awareness among providers of the risks prevalent on their respective platforms and for taking proportionate measures.

A realistic assessment of the risk review acknowledges that providers may, whether intentionally or inadvertently, fail to adequately assess or downplay the risks order to avoid implementing undesired measures. Effective countermeasures are necessary to address this issue:

- Relevant providers of online platforms should confidentially submit their risk reviews to the competent supervisory authorities (while maintaining the provider's significant business secrets, which are to be excluded from this). This requirement also applies to any relevant changes or adjustments of the security concept.

- To enable continuous oversight, the responsible supervisory authorities should have the ability to confidentially review the risk reviews at any time, while respecting the company's protected business secrets as outlined above.

- The assessment of proportionality is a value judgment that can vary significantly depending on the individual case. Therefore, the balancing aspects in the risk review should be presented in detail and made accessible to ensure that the provider's perspective is adequately considered.

More guidance is also necessary for the continued development of the review process. While the guidelines address many important levels of analysis, the broad scope for interpretation of certain elements – such as the likelihood of minors accessing the service – carries a risk of arbitrariness. It would be beneficial to examine all open-ended requirements with the aim of providing clearer and more specific options for their interpretation and application.

Orientation towards the 5C typology is useful in the context of the risk review. However, it remains unclear which concrete steps should be regularly undertaken when one or more risks identified by the typology are present.

Although this will always be a matter for case-by-case assessment, minimum requirements should be formulated. For example, along the lines of "unless there are compelling reasons in the individual case that speak against the application of the measure, the following measures should be taken for the risk from the 5C typology (e. g., "contact")."

Prior to the Digital Services Act, the Federal Agency for Child and Youth Protection in the Media conducted provider oversight and assigned typical measures to be taken in certain risk constellations, without prescribing them definitively. This assessment criteria could be used to create uniform standards to guarantee orientation regarding an effective risk review.

III. Service Design

Age Assurance

KidD welcomes that the Commission has highlighted age assurance in the guidelines as an important tool for ensuring child and youth media protection and is further aligning them with the aforementioned basic principles. The basic principles should address not only options available for children to circumvent age restrictions but also the possibilities for adults to create accounts posing as children and thus attempting to access protected areas.

The draft rightly identifies high risks for minors, particularly regarding content such as pornography. KidD concurs with the necessity of effective age assurance when it comes to harmful content. The risks arising from the use of different functionalities on various social media platforms should also be highlighted when it comes to the risk analyses and the corresponding need for proportionate effective age assurance mechanisms. Children and young people are often confronted with (age-) inappropriate or dangerous interactions. Where inappropriate or harmful content to minors is offered or inappropriate or harmful interaction is possible, serious age assurance is required. It is also important to consider the different perspectives of age verification, especially with regard to its developmental potential: effective age assurance can enable safety settings by default, thereby creating safe online spaces for minors that remain inaccessible to adults.

When an online platform grants access to content labeled as “over 18”, it should have a certified age verification system in place. This requirement aligns with German law, which mandates closed user groups for potentially harmful, yet legal content. The paramount importance of effective age verification was recently strongly emphasized by the joint federal and state competence center *jugendschutz.net* in its annual report: Reliable age verification is more often necessary during registration to enable meaningful adjustment of precautionary measures. Only in this way can different protection needs be met based on age. Social media increasingly uses estimates, but these should be critically examined due to the associated need for analysis over a longer period of time.

As valuable as age assurance is, each age verification measure must meet clear requirements to justify even relatively significant infringements of users' fundamental rights.

The Commission presents a system and corresponding requirements for age verification.

Regarding age estimation, the specific requirements should be applied in detail. Clearly, more guidance through further specifications is needed here to avoid the associated extensive data collection and to guarantee effectiveness. It would be welcomed if the Commission, in this particularly sensitive area of data processing, described clear requirements for the systems to be maintained that enable such estimations in a legally compliant manner.

It is also important to maintain a balance between protection and inclusion/participation.

Platform providers should be obliged to provide a system allowing users to indicate whether their own user-generated content is suitable only for adults. The provider needs to inform the users of this obligation and give information which content is considered to be adults only. Age rating systems should be used on platforms to classify content for various age target groups and indicate which content is appropriate for which age group. In addition, easily accessible functionality enabling users to report incorrect age ratings quickly and without significant effort, regardless of whether these adult ratings are generated unintentionally or with malicious intent. This should include age-appropriate reporting and follow-up control mechanisms. AI tools could also be utilized to identify incorrect ratings.

Registration

KidD fully agrees with the statements regarding registration. In the absence of registration, it should be assumed that users may be minors, and accordingly, appropriate security must be implemented.

Account settings

The Federal Office welcomes the requirements set out in this section, which aim to protect the identity and integrity of minors.

It should be clarified that in the absence of registration, users should always be assumed to be minors by default, and thus the highest security requirements should be applied.

Furthermore, the case groups referenced in lines 422 and 423 require further specifications.

Finally, there is no explanation as to how the interaction between parental controls, default settings, and other potential measures can be meaningfully organized. This is particularly

relevant for time management tools and other protective mechanisms, such as spending-limits.

In particular, the extent to which children and young people can override security settings themselves, for example through providing consent, should be elaborated upon. Taking advancing age and opportunities of minors into account will be crucial in this context. A solution is needed to enable age-appropriate access for different age groups below the adult staged, as well as to determine which functionalities should be enabled accordingly. Therefore, the Commission should provide more detailed guidance in this area in particular. For instance, it remains unclear how age-appropriate warning signals should be technically implemented or which measures can be put in place against excessive use.

Online interface design and other tools

Particularly intrusive design elements should be described in greater detail, especially for platforms aimed at children and young people, which are often characterized by visually intense and graphically rich designs.

Recommender systems and search features

If the platform can, in principle, also be used by minors, it is necessary to clarify under what conditions behavioural data may be collected. Age-differentiated designs allow more self-determination for older minors.

The security risks identified in section 552 should be further detailed and specified, for example in a footnote. The reference to “unrealistic beauty ideals” is too vague. The BzKJ has published a compendium *Gefährdungsatlas* that captures the most relevant risks while taking actual usage behavior into account.

Additionally, it is necessary to provide clear criteria for when content is considered to be repeated in a problematic manner.

Commercial practices

The definition of lootboxes and gambling-like features should be sharpened to provide better guidance for providers and regulators regarding a proportionate exclusion of these elements.

Moderation

It is essential to emphasize the importance of child-friendly moderation. Article 28(1) DSA extends well beyond the basic requirements set out in Article 16 DSA. We would also like to expressly emphasize that the clear and transparent definition of moderation standards should ideally be developed in collaboration with experts.

Reporting, user support and tools for guardians

It should be clarified that legal remedies and external assistance (e. g. as a result of moderation decisions), especially for children and young people, should be offered in a format and language appropriate for them and easily accessible. As far as law enforcement is concerned, opportunities for external assistance must be offered to obtain further assistance.

User reporting, feedback and complaints

As young people's capabilities develop, parental control should be gradually limited. This raises the question of how age-appropriate accommodations can be effectively managed through age verification. Crucial details on this matter are currently lacking (see above).

Live streams are difficult to control when it comes to risks. For this reason, time-shifted streams should be considered if possible.

KidD supports in principle all other statements, notably the “User support measures” and “Tools for guardians”.

Governance

The Federal Office highly welcomes the emphasis on establishing clear responsibilities accompanied by sufficient resources and authority. While staff training may be difficult to supervise directly, the provider's competence is a key prerequisite for ensuring the implementation of adequate measures.

Terms and conditions

To avoid misunderstandings, the relationship to Article 14(3) DSA should be described in more detail. At the same time, the section could also provide many important statements regarding the specification of Article 14(3) DSA.

Monitoring and evaluation

Clear time frames should be specified in all respects.

Transparency

Transparency requires an age-differentiated approach. Further details are required on how this should be organized. In this section in particular, vague terms – e. g. relevant information – should be formulated much more clearly.

Contact

Contact information for general inquiries: info@kidd.bund.de

Head of KidD: Michael Terhörst, Michael.terhoerst@bzkj.bund.de

Internet: www.kidd.bund.de