USK Unterhaltungssoftware Selbstkontrolle

Statement by the Entertainment Software Self-Regulation Body (USK)

On the draft 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.

About the USK

The Entertainment Software Self-Regulation Body is a voluntary organization within the games industry. It reviews digital games and assigns them an age rating in Germany. It also highlights any potential content and usage risks for children and young people. The USK is recognized as the responsible self-regulation body under both the Federal Youth Protection Act and the State Treaty on the Protection of Minors in the Media. Numerous companies have joined the USK as members in order to cooperate closely and on a permanent basis on the issue of youth protection. The USK is also a co-founder of the IARC system (International Age Rating Coalition). In addition, the USK is involved in media education and publishes a parents' guide, as well as other materials. The USK is advised by an advisory board, which, among other things, defines the USK principles and the guiding criteria for the ratings. Further information: www.usk.de

Introduction

The USK expressly welcomes the opportunity to submit comments as part of the public consultation on the European Commission's guidelines pursuant to Article 28(4) of Regulation (EU) 2022/2065 (Digital Services Act). The USK sees the public consultation on the guidelines as an important opportunity to contribute practical experience and examples of proven measures.

The USK has 30 years of extensive expertise in the field of protecting minors in interactive entertainment services. It is not only responsible for age ratings of games and apps in Germany, but also certifies technical solutions for the protection of minors provided by providers in accordance with German law.

From the USK's perspective, the following points are particularly noteworthy with regard to the EU Commission's guidelines:

- **Disproportionate focus on age assurance**: Age assurance measures remain the focus of the guidelines, even though, according to the basic understanding, other measures should also be considered as proportionate solutions. However, against the background of the principle of data minimization, a focus on age assurance measures is questionable. “Tools for Guardians” or parental control tools offer a very high level of protection while also ensuring data minimization. Furthermore, only parental controls allow for detailed and gradual adjustment of protective measures in a proportionate manner, thereby guaranteeing participation rights.
- **Non-consideration of self-regulatory approaches**: In particular, age ratings such as those assigned by the IARC system provide important guidance and increase the level of protection and transparency (awareness and possibility of age-appropriate filtering) by taking into account content and usage risks and providing additional information. These proven international and national protective mechanisms are not adequately taken into account in the current draft guidelines.
- **Insufficient consideration of parental control systems:** Parental control systems form the indispensable basis for any further measures. They enable minors to participate safely and in an age-appropriate manner on online platforms while at the same time preserving the educational rights of parents. Parental controls are an established and effective measure in Germany to ensure that minors have access to age-appropriate content. Youth protection programs are tested and certified according to legal criteria by state-recognized self-regulation bodies.

I. Scope of the Guidelines

Although the draft guidelines comment on the scope of application of the guidelines, they do not sufficiently clarify when a service within the meaning of Recital 71 DSA is to be classified as "directed to minors" or "predominantly used by minors". Without a clear definition or guidance, it remains unclear when the relevant obligations apply to a platform. The Commission needs to provide more specific guidance in this regard.

II. Non-consideration of self-regulatory approaches

In the USK's view, there is clearly unused potential in the lack of consideration of proven effective models for preventive, self-regulatory approaches. For example, service providers in Germany are subject to comprehensive youth protection regulations and implement the relevant requirements in cooperation with recognized self-regulatory bodies. Such or similarly developed and proven procedures are largely ignored in the draft guidelines, even though recognized self-regulatory bodies make a substantial contribution to the legally compliant implementation of youth protection duties in cooperation with their member companies. Thanks to their technical expertise, they play a key role in developing and establishing reliable minimum standards. These standards serve as practical guidelines for providers, create clear expectations, and contribute to the coherent and transparent application of the law. The role of such bodies is in line with the internationally established understanding of a participative, multi-stakeholder model of youth media protection, as expressed, among other things, in the recommendations of the United Nations (see UN Committee on the Rights of the Child, General Comment No. 25 (2021), Section V, "C. Coordination," No. 27). Against this background, cooperation with qualified self-regulatory bodies such as the USK is an appropriate and responsible mechanism for fulfilling regulatory obligations under the Digital Services Act.

With regard to potential risks, age ratings in particular are completely ignored in the guidelines. Age ratings provide key guidance for parents, educational professionals, and minors themselves. In this context, the automated rating system of the International Age Rating Coalition (IARC) should be highlighted. This system is the result of international cooperation between self-regulatory institutions and has been state-approved and legally recognized in Germany. Age ratings that, in accordance with German youth protection law, take into account not only content risks but also usage risks and precautionary measures in the context of age rating and provide appropriate additional information on the functionalities contained and the main reasons for the age rating, significantly increase the level of protection and also contribute to the required transparency (see 8.4 of the draft guidelines). Usage risks include, for example, communication and contact risks, elements that promote excessive media use, gambling-like mechanisms, and other features that may impair the ability for self-regulation ("dark patterns"). The sensitizing effect of age ratings is particularly effective in combination with technical protection mechanisms such as parental controls (youth protection filters), which create age-appropriate access options.

Effective and already established international and national self-regulatory protection mechanisms and procedures for the protection of minors on online platforms are therefore not sufficiently taken into account.

III. General Principles and Risk Review

The USK welcomes the EU Commission's approach of explicitly mentioning the principle of proportionality and children's rights in the framework of the general principles. Nevertheless, the right to play (cf. Art. 31 of the Convention on the Rights of the Child) is not explicitly mentioned in the section “General Principles” (see p. 159 ff.) alongside “the right to protection, non-discrimination, inclusion, participation, privacy, information, and freedom of expression.” The USK believes that this right should be emphasized more clearly in the context of the proportionality of measures. In this way, aspects such as participation in leisure activities and play could be given equal consideration.

The guidelines are also primarily based on the highest standards of protection and thus on the youngest users. Ultimately, this does not live up to the guidelines' own claim (see in particular lines 193 ff. of the guidelines) to provide practical guidance that enables the implementation of children's rights in a balanced manner by specifically naming various options for action. In particular, a comprehensive age-differentiated approach is missing. For example, the participation and self-determination rights of older adolescents are not sufficiently taken into account, even though they have different needs and skills that must be considered in relation to the use of digital services, which the guidelines should also reflect.

From the USK's point of view, there is a particular lack of clear connection between risk assessment and specific measures to mitigate risk. This means that an essential component of the risk review is not taken into account and the guidelines appear too vague overall. This could lead to considerable legal uncertainty and make reliable implementation in practice more difficult. In particular, it remains unclear which specific protective mechanisms are expected for each type of risk and how the measures are to be weighted and balanced against each other so that they are not criticized as inaccessible or ineffective solely on the basis of their sheer number. The actual goal of providing providers with clear and comprehensible recommendations for meeting regulatory requirements thus remains incomplete.

To ensure consistent and practical implementation, it would be useful to systematically compare the identified risk types in each of the five risk categories (5Cs) with the risk mitigation measures specified in the guidelines. Such a structured approach could provide platform providers with reliable and practical guidance. The description should clearly emphasize the recommendatory nature of the guidelines, while at the same time making it transparent where certain minimum standards apply and where flexible, risk-appropriate solutions are possible. In addition, providers should continue to be given sufficient flexibility to adapt measures to the specific characteristics of their platform and the needs of their underage user groups.

IV. Age assurance

Particularly with regard to age assurance, the structure and interconnection of the measures and the overall objective of the guidelines remain unclear. In view of the principle of proportionality explained at the beginning of the guidelines, age assurance should be an option, but in the context of the guidelines' specific provisions, this seems to be an almost inevitable requirement. This creates a tension between the desired openness to different protective measures and the actual prioritization of age assurance systems. There are also no clear indications as to the conditions under which alternative protective measures can be used instead of age assurance.

It is particularly important to note that not all risks to minors are addressed equally effectively or proportionately by age assurance measures. Behavioral risks, for example, depend less on the biological age of users than on social interactions and the structural framework of the respective platform. Simply knowing a user's age has no influence on the specific behavior of minors. Age assurance systems do not prevent the disclosure of personal information or risky or excessive usage behavior in the digital space.

From the USK's point of view, it is therefore necessary, particularly in the case of so-called “medium risk” content, to take into account other technical measures of equivalent effectiveness in addition to age estimation. These include access restrictions that are not necessarily based on age estimation, such as youth protection programs. Such youth protection programs, which are recognized in Germany by self-regulatory bodies in accordance with legal criteria, ensure a high level of protection by reliably adapting access to content to the age level specified by parents and at the same time providing effective barriers against attempts to circumvent them. This means, for example, that children cannot simply set up a “fake” profile. At the same time, such programs enable parents to tailor the protection settings in detail to the age and abilities of their child.

It is still necessary to specify what the EU COM actually means by “medium risk.” Although there are some indications (lines 284-289), it would be important to provide more concrete examples. This would help to define the risks for which alternative measures could be considered proportionate.

The current approach of linking the need for an age verification system (AVS) to the age specified in the terms and conditions fails to meet the protective purpose of Art. 28(1) DSA. The age limit specified in the terms and conditions may also be based on liability or contractual considerations and is not necessarily related to the specific risks for minors. Therefore, the focus should be solely on the actual risk of impairment or endangerment of the personal integrity of minors.

The EU Wallet Standard approach does offer a way to standardize age verification. However, the design of this standard should be open enough to allow for the integration of alternative methods that are established and recognized in the respective member states. An overly rigid standard could unnecessarily restrict the diversity of proven national solutions and unnecessarily displace established and effective solutions.

V. Default Settings

Section 6.3.1 emphasizes the central importance of default settings as a protective mechanism for minors and suggests that this should be a proportionate alternative to age assurance (“providers...that use default settings to ensure a high level of...”). However, it remains unclear whether a platform that treats all users as minors by default - i.e., applies particularly strict default settings - also implements the requirement of Art. 28(1) DSA without age assurance, although there are several references to this (e.g., line 389 ff.).

It should also be explicitly clarified whether default settings alone are sufficient to counteract risks to minors without having to use age assurance methods. If the Commission recognizes default settings as an equivalent alternative to age verification or “age estimation,” this should ideally be clarified at the beginning of section 6.3.1. It should also be made clear in which cases default settings are usually sufficient and when additional measures are necessary. In order to highlight the high importance of account and default settings in the system, the entire section should be moved to the front.

The default settings listed in section 6.3.1 are predominantly framed from the perspective of younger children. However, there is a lack of differentiated consideration of the rights, needs, and abilities of older children and adolescents. They have a wide range of media experiences and, with increasing age, possess the competence to distance themselves from risks and make conscious decisions. Consequently, adolescents in particular have a need for greater autonomy, for example with regard to the visibility of content or interactions. In order to strike the right balance between protection and participation, the default settings need to be more refined.

This could be achieved by linking the default settings to parental control tools. Parental control tools offer the option of activating central protective measures and, if necessary, making individual adjustments to ensure age-appropriate and safe use. In addition, such a link can prevent underage users from changing these settings on their own.

There is also no explicit clarification that the requirements in section 6.3.2 (“Account Settings”) expressly refer to accounts belonging to minors. This distinction is crucial in order to correctly classify and implement the requirements in 6.3.1 (Default Settings).

VI. Commercial Practices

There are substantive overlaps with consumer protection law. From the USK’s perspective, a clear distinction between the two legal areas should be maintained in accordance with their respective protective purposes, in order to avoid deepening the risk of diverging legal developments due to overlapping regulations. It is important to emphasise that, in the view of the USK, very few providers of gaming platforms qualify as online platforms within the meaning of Art. 3 (i) of the DSA and are therefore subject to the obligations set out in Art. 28(1). As a result, the specific requirements addressed here - particularly those concerning loot boxes - will apply to only a very limited number of cases.

Overall, the current wording regarding loot boxes exceeds the principle of proportionality. The generalisation of loot boxes as generally problematic or inadmissible for minors fails to take into account the necessary differentiated assessment. What matters is the specific design and integration of loot boxes within the game, as well as the balance between potential risks and existing protective measures. Moreover, loot boxes typically constitute “own content” and therefore do not fall within the scope of the DSA. In Germany, such monetisation practices are addressed in the context of child and youth media protection through the age rating process, either via assessment by independent committees or through the globally used and state-recognised automated classification system IARC (International Age Rating Coalition). In both systems, such game mechanics are taken into account during age classification and are indicated with additional descriptors. These balancing processes are thus already reflected in the German regulatory framework and have proven highly effective in the context of USK procedures, which include direct involvement of state authorities.

VII. Tools for Guardians

From the USK's point of view, there is a need for a much stronger recommendation for the systematic use of parental control tools. Parental controls are an effective means of protecting minors from the risks associated with the use of digital platforms. They enable age-differentiated settings to be made and allow for individual adjustments by parents. Compared to age assurance via age verification or age estimation, they offer the possibility of enabling younger users to participate in platforms in a safe and

age-appropriate manner. This aspect of participation, as well as the parental privilege enshrined in German constitutional law (Art. 6 GG), is not sufficiently taken into account in the existing recommendations and should be emphasized much more strongly in the guidelines.

What is needed is a clearer commitment in the guidelines to “tools for guardians” or parental controls, which are designed in a way that hat recognizes their importance and creates a corresponding incentive for service providers. These are a long-established and effective tool – also in German legislation – for protecting children from harmful content while ensuring safe participation. It should therefore be added that youth protection programs can guarantee a high level of privacy, security, and protection for minors, especially if they have been tested and certified by independent experts from a self-regulatory body in accordance with criteria laid down by national law.

The existing separation between parental control tools and default settings should be reconsidered. In practice, these functions are closely linked. Access to content, chat functions, or output restrictions are often organized via default settings within a parental control tool. Parents can adjust these as needed. Separating the two aspects therefore does not reflect how they actually work. An adjustment is absolutely necessary.

The use of automated rating systems for age classification of content should be considered as a further measure within the framework of the recommendations. The IARC (International Age Rating Coalition) system, which is recognized internationally and in accordance with national regulations applicable in Germany, offers an established solution for this purpose that is already used by numerous large platforms. The system is based on self-disclosure by providers via a standardized and curated questionnaire, which is then evaluated on a country-specific basis using a culturally sensitive matrix. The results are subject to further quality assurance measures. In practice, IARC already serves as the technical basis for USK-approved youth protection programs on consoles to filter inappropriate content according to the set age level and block it from being played.

Youth protection programs play a central role in German youth media protection regulations. Particularly noteworthy is the possibility of having youth protection programs recognized or certified by recognized self-regulatory bodies such as the USK in accordance with legal requirements (§ 11 JMStV). The programs are checked for filter rates and the possibility of circumvention, among other things. Certifications of youth protection programs according to national, legal criteria by independent experts from a state-recognized voluntary self-regulation body should be taken into account.

VIII. Transparency

Age ratings and additional information or descriptors are not taken into account at all, even though these have been proven to be an essential measure for providing guidance and raising awareness. Age ratings are not only assigned or generated by the platform, but also by users as part of a self-classification system for user-generated content (cf. IARC ratings in Fortnite).

Regardless of the labeling of individual user-generated content, however, the age rating of online platforms per se (e.g., social media apps or game creator platforms via the IARC system), including their legal implications and consequences, must also be taken into account in the impact assessment pursuant to Art. 28(1) DSA. Age ratings and additional information on the functionalities contained in the apps and the main reasons for the age rating already raise awareness of the general relevance of the

platform as such for the protection of minors. Under German youth protection law, the assessment also takes into account usage risks and precautionary measures in relation to these risks.

Furthermore, age ratings provide the basis for age-appropriate access. Only the age rating of digital content/environments enables the platform to make age-appropriate functions and/or content accessible, for example after an implemented age assurance.