European Commission Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

ISFE Position

November 2022

1. Every child has the right to be respected, protected and empowered online and offline. Children have the right to play, to create and to actively participate in the community through digital inclusion and, importantly, children have the right to protection and privacy.

2. With more than 52% of Europe's population playing video games across all age groups, and with playing video games being a popular pastime for children, the video game industry is committed to a fun and safe video game play environment.

3. Online video game play is among the safest online activities that children can participate in.[1] Most video games do not allow interactivity outside the game play environment, and the in-game communications, i.e. chat functionality, utilise a range of tools to protect players, depending on the risk. Developed over a period of more than twenty years, the video game sector has a solid framework prioritising minor protection, based on its commitment to keep online gameplay interaction free from illegal content and content that may be inappropriate for children.

4. This paper explains (i) what type of online interactions occur in videogames, (ii) how the video game industry prioritises children's online safety, and (iii) our recommendations to the Commission's proposal.

What type of online interactions occur in video game play?

5. The purpose of in-game communications is to allow players to collaborate, to talk about the game play and to replicate the feel of playing physically with friends but in an online environment. Communications between players in video games are typically restricted, ephemeral, filtered, reportable, pseudonym-based and can be deleted and turned off.

    - **In-game communication** features are largely text based but can also include voice chat. In-game communication with other players facilitates collaboration and conversation about game play, and enhances the game-playing experience; e.g. discussing strategies. These communications tend to be short. Furthermore, they often take the form of real time chat that is visible (or audible) to all the players of the game. It is rare that in-game communications allow for photos and videos to be exchanged, or indeed, offer the technical possibility to do so. For some companies, this is actually prohibited in their terms and conditions.

    - **At video game platform level,** additional communications features may be offered but, in the majority of cases, these features are used to share image and video captures of the gameplay itself.[2]

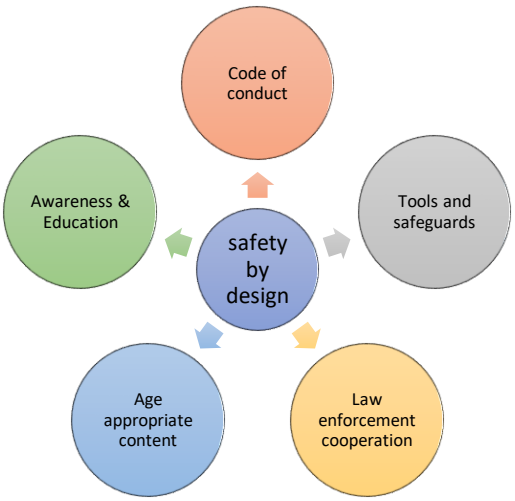
[1] Annex Reports and studies.

[2] Where the sharing of user-generated content via photos, video or streamed content is permitted, Proactive Image Detection such as PhotoDNA is typically used, which is a robust image hash detection technology allowing operators to reliably identify and remove known CSAM

- **In-game communication is different to adjacent communication tools.** Separate communication companies, such as Discord, are different to video game companies. They allow for exchanges during gameplay but these tools are not provided by the video game publisher or the platform on which the game is played and are therefore not under their control. They are dedicated communication platforms and should be approached as such.

How does the video games industry prioritise children's online safety?

6. Because of the popularity of video games among children, the sector committed early on in its history to a safe gameplay experience. Developed over a period of more than twenty years, the video game sector has a solid framework to prioritise safe online gameplay, for both adults and children based on its commitment to keep online gameplay interaction free from illegal content and content that may be inappropriate for children. Members take various actions and employ a number of tools that have been in place for many years, and that are best practice examples for other sectors. Together, these tools constitute a **safety-by-design** approach also when in-game communications are involved.



i. **Age-appropriate content**: The Pan European Game Information System (PEGI) ensures that a video game is assessed according to its age appropriateness based on criteria used by independent evaluators including, for example, bad language, violence or sexually explicit content. Following this evaluation, an age rating is attributed to the game. This enables parents to choose a game that is appropriate for the child. PEGI is a voluntary, and in some countries, a co-regulatory system adopted into national law. Currently 38 countries use the PEGI system.

ii. **A Code of Conduct:** In addition to receiving age ratings for their games, video game companies are contractually bound by the PEGI Code of Conduct. Article 9 of the Code introduced in 2007, **focuses on safe online gameplay environments** where online interaction is offered. It stipulates that signatories should keep any user-generated content free of content which is "*illegal, offensive, racist, degrading, corrupting, threatening, obscene or that might permanently impair the development of minors*". The Code also requires appropriate reporting mechanisms to be in place to allow players to notify such content or any type of inappropriate conduct.

iii. **Tools and safeguards:** A variety of tools and safeguards are used to protect minors from potentially harmful or illegal content. In the game itself, where communication between players is possible the player may typically have access to tools that allow reporting, blocking and muting, among other functions. Filtering, including proactive filtering, is commonly used, such as profanity filters and tools that obfuscate links to third party sites. Depending on the nature of the service, moderation tools are often deployed and human moderation used to identify and to remove harmful content and to remove and report illegal content to law enforcement. For some video game specific UGC platforms, pre-moderation of text chats is used for games that are particularly popular with children, where, for example, private information is hashed out prior to upload, as children may not always understand

the risks associated with sharing contact details. **Parental control tools** enable parents to restrict communication with others both in-game and at platform level to ensure that children are protected from, for example, solicitation from unknown players[3]. These tools can be used on the web or within mobile apps, as well as on console, to further facilitate ease of use by parents and guardians. On some platforms, when parents permit communication with other players in the game, parents can still pre-approve communications requests from existing friends of the child. On some platforms, a parent can permit the child to use communication features in one game without affecting the setting that blocks communication in all other games played by the child ("whitelisting"), which gives parents the ability to choose what is right for their child. **Community guidelines:** many platforms and online games have established community guidelines that set out expectations for appropriate player behaviour in their online ecosystem and provide information on the recourse that may be taken in the event of violation of guidelines.

iv. **Cooperation with law enforcement:** Where illegal content is detected, either via user reports or through moderation systems, members companies will remove content, review it and escalate to law enforcement. Individual member companies of ISFE cooperate directly with civil society organisations such as INHOPE, ECPAT, NCMEC (as a proxy for law enforcement) and WePROTECT.

v. **Awareness and Education:** Educational efforts aimed at players of all ages, parents and educators are crucial and a major component to achieve safe online environments. ISFE and members have put in place initiatives across Europe in national languages providing information about tools, tips, and suitable games, to ensure that parents are aware of what is available to manage their child's online activity and game play to ensure that it is safe[4]. The most effective way to ensure online safety is that governments support industry initiatives that focus on education and awareness raising.

Comments on the proposal

7. A safe online gameplay experience is a key priority for the video games industry and our sector is committed to the European Commission's goal to fight child sexual abuse online effectively.

8. Successful regulation should allow for clear reporting requirements applicable to all providers who become aware (actual knowledge) of potential child sexual abuse on their platforms. Where additional obligations are deemed necessary, these should be proportionate in relation to the risk that the particular communication service may pose and ensure that their interference with the fundamental rights to privacy and data protection remains lawful.

   Considering the low prevalence of CSAM and solicitation in in-game communications, and the limited opportunities to share images and videos, ISFE is concerned that the proposal goes beyond what is strictly necessary and proportionate and therefore could negatively impact the essence of the rights guaranteed in the Charter of Fundamental Rights. Such intrusion would constitute an interference with the confidentiality of communications that does not comply with the requirements of Article 52(1) of the Charter[5]. ISFE urges caution against a one-size-fits-all approach that treats games like

[3] Acccording to a recent Ipsos survey 60% of parents do not allow children to play muliplayer online games. Among the 40 % of parents that do allow exchanges with other players, 80 % of parents supervise the online interactivity.
[4] Responsible Gameplay - ISFE ; ISFE-EGDF_Call-for-feedback-BIK-Strategy-28-10-2021.pdf
[5] Charter of Fundamental Rights of the European Union (europa.eu)

other, higher-risk digital platforms, or imposes the same expectations on companies, regardless of risk.

9. This is supported by Recital 5 of the proposal which states that "*given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner*".

10. As recognised by a number of reports and studies (see the Annex to this proposal), online video games are some of the safest places for children to be connected to the internet, in particular because of the minor and ancillary feature nature of online communications in video games, which are largely text based, but also because of the many tools and safeguards in place, as detailed in the previous section.

11. Despite the intention of the Regulation to apply differentiated obligations, the definitions in the proposal are tied to a number of obligations which do not consider the nature of the service, nor the prevalence of harmful content of a service being misused. ISFE therefore recommends that the proposal for a Regulation considers the following seven points:

12. **Proportionate obligations according to the nature of service and prevalence of misuse**:
    a. In-game communications/chats, where they are ancillary to the core service should not be included in the definition of interpersonal communications services in Article 2 (b), supplemented by Recital 5, as this definition triggers disproportionate risk assessment obligations in Article 3, risk mitigation measures in Article 4 and risk reporting obligations in Article 5. These do not suit services which are most often text based, and at low risk for being misused for child sexual abuse. This approach is at odds with Recital 5 which states that "*the obligations imposed on the providers of those services should be differentiated in an appropriate manner".*
    b. Recital 12 states that child sexual abuse material "*typically consists of images or videos*". Therefore, hosting services that do not allow user generated photo or video sharing should not be subject to the risk assessment in Article 3 and risk mitigation in Article 4.
    c. Because of (i) the safety by design approach already in place for in-game chats and online communications at video game platform level, and (ii) the necessity for risk assessments to be proportionate and reasonable, according to the nature of the service and the risk of abuse, in-game communications and communications at platform level should not be subject to obligations related to Articles 3 (risk assessments), 4 (risk mitigation measures) and 5 (risk reporting). Instead they should be required to comply with reporting obligations in Articles 12 and 13 when they become aware (actual knowledge) of potential child sexual abuse on their platforms.

13. **Detection of solicitation of children and unknown material should be excluded from the scope of the Proposal:** In light of the concerns raised by the EDPB and EDPS in their joint Opinion[6] regarding interference with the protection of fundamental rights to privacy and the protection of personal data, detection of unknown material and solicitation of children should be excluded from the scope of the Proposal.

[6]Ibid., §76, 91

14. **Support the development of technologies that can address CSAM in a lawful manner:** Considering the nascent state of technologies available to deal with new CSAM and solicitation of children and as stated in the joint EDPB-EDPS opinion, existing technology remains insufficiently developed and inaccurate. The Commission should rather encourage development of technological solutions to ensure that providers have a variety of robust solutions to choose from.

15. **Parental control tools should be recognised as a form of age assurance.** The obligation to use age verification and age assessment measures to 'reliably' identify child users on their services (*Article 4.3*) does not take into account the limited tools currently available on the market. Some of these tools rely on methods which themselves raise privacy concerns or may result in over-blocking such as the exclusion of young-looking adults from accessing online services. Parental controls are a form of account confirmation that give functional age assurance. In this context, ISFE welcomes the recommendation in the joint EDPB-EDPS Opinion to expressly allow providers to rely on parental control mechanisms in addition, or as an alternative, to age verification.[7]

16. **The EU should continue to support voluntary detection of CSAM**, as called for in the joint EDPB-EDPS Opinion. [8] The Proposal should continue, not discontinue, the voluntary use of technologies for the detection of CSAM. The added value that the current interim regulation brings in allowing voluntary measures, subject to safeguards, to combat and prevent CSAM should continue to exist.

17. **The EU should look at how global coordination can be ensured** by harmonising existing standards and obligations on CSAM detection and removal at international level while maintaining a high level of protection.

18. **The need for harmonised data on trends**: Public entities that receive reports of CSAM should publish data annually to allow for the better understanding of trends, of how overall efforts of stakeholders are producing positive results, and to better target additional measures that may be required.

---

[7] joint Opinion 04/2022 on the draft proposal for a regulation laying down rules to prevent and combat child sexual abuse (CSAM), §92.

[8] joint Opinion 04/2022 on the draft proposal for a regulation laying down rules to prevent and combat child sexual abuse (CSAM), §19-21.

***ANNEX* - Reports and studies**

- a 2020 survey commissioned by the UK's regulator, Ofcom and the ICO, of ca 4000 adults and children aged between 12 and 15, reported that 62% of adults and 81% of children had experienced potential online harms in the previous 12 months. Compared to other digital platforms sources (social media, instant messaging, video sharing), gaming sites and platforms were the least cited by respondents for potential harms, with 2% of adults and 3% of children experiencing such harms via online gameplay.
- a 2020 Interpol report highlighted increases in CSEAM-sharing via P2P and in exchanges and discussions on the darknet, that viral distribution had increased on social media, and viral video circulation via messaging apps. As regards video game platforms, countries reported "*no significant changes in the volume of cases (reported) of children being targeted by sexual offenders"*.
- NCMEC's 2021 Cybertipline report by Electronic Service Providers showed that CSAM and grooming instances for video game companies were considerably lower than other platforms that have as their primary purpose photo/video sharing and communications features.
- The Radicalisation Awareness Network 2020 conclusions paper stated that that grooming and extremist content is rare in in-game communications but is more frequent on adjacent gaming communications platforms.

Contact:
Ann Becker, Head of Policy and Public Affairs, ISFE: ann.becker@isfe.eu
Jürgen Bänsch, Director Policy and Public Affairs, ISFE: juergen.baensch@isfe.eu

About ISFE
www.isfe.eu

The Interactive Software Federation of Europe (ISFE) comprises national trade associations covering 18 countries throughout Europe which represent in turn hundreds of games companies at national level. ISFE also has as direct members the leading European and international publishers, many of which have studios with a strong European footprint, which produce and publish interactive entertainment and educational software for use on personal computers, game consoles, portable devices, mobile phones and the Internet.

The video games industry represents one of Europe's most compelling economic success stories, relying on a strong IP framework, and is a rapidly growing segment of the creative industries. The European digital single market area is the third-largest market for video games globally. All in all, there are around 5,000 game developer studios and publishers in Europe, employing over 98,000 people.