30.9.2024

EGDF RESPONSE TO THE CALL FOR EVIDENCE ON THE DIGITAL SERVICE ACT GUIDELINES TO ENFORCE THE PROTECTION OF MINORS ONLINE

About EGDF

1. **The European Games Developer Federation e.f. (EGDF)**[1] unites 24 national trade associations representing game developer studios based in 22 European countries: Austria (PGDA), Belgium (FLEGA and WALGA), Croatia (CGDA), Czechia (GDACZ), Estonia (Gamedev Estonia), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Lithuania (LZKA), Netherlands (DGA), Norway (VIRKE Produsentforeningen), Poland (PGA and IGP), Portugal (APVP), Romania (RGDA), Serbia (SGA), Slovakia (SGDA), Spain (DEV), Sweden (Spelplan-ASGD), Switzerland (SGDA), Turkey (TOGED) and the United Kingdom (TIGA). Through its members, EGDF represents more than 2 500 game developer studios, most SMEs, employing more than 45 000 people.

2. **The 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. In 2023, there were around 5 300 game developer studios and publishers in the EU, employing over 90 000 people and running a combined turnover of over €19bn[2]. In 2023, Europe's video games market was worth €25,7bn, and the industry has registered a growth rate of 5% in key European markets[3]. The European digital single market is the third-largest video game market globally.

3. **The European video games sector takes its responsibility to ensure a fun, safe, inclusive and responsible gameplay environment for minors very seriously.** Video games are played by children and adolescents across Europe. The sector is aware of the challenges related to the protection of minors in the digital environment. It abides by strict European laws on data and consumer protection and supplements this with its self- and co-regulatory standards through the Pan-European Game Information System (PEGI), which is a model of successful self- and co-regulation and is today deployed in more than 35 European countries.

[1] For more information, please visit www.egdf.eu
[2] EGDF-VGE 2023 European games industry insights report https://www.egdf.eu/wp-content/uploads/2024/06/2022-European-video-games-industry-insight-report.pdf
[3] ISFE-EGDF 2023 Key Facts https://www.videogameseurope.eu/publication/2023-video-games-european-key-facts/

1. Summary of EGDF contribution

4. **The Commission must take a human rights-centric approach to drafting the guidelines on the protection of minors.**

    a. **By principle, platforms should evaluate and balance all their policies on content and services allowed on their platforms from the perspective of fundamental rights and freedoms in the EU**. This includes, for example, protection of minors from harmful content, protection from discrimination, right to privacy and securing their access to culture, as well as freedom of arts and expression, free movement of services on the digital single market area and freedom to conduct business. The same principle applies to the Commission while it is drafting the guidelines.

    b. **As underlined by the UN Convention on the Rights of the Child, the guidelines must empower parents to take care of their responsibility for the upbringing and development of the child.** The Commission must ensure that the guidelines ensure that parents, not platforms, have the primary control over, e.g., digital artistic content their children can access and the personal data of their children.

    c. **The Commission guidelines must carefully ensure they respect children's right to leisure and participation in cultural life.** It is important to ensure that the protection of minors' practices does not just empower parents to make informed decisions; they must also empower children to make informed decisions in their digital lives.

    d. **The Commission should approach the protection of children from both the perspective of children as consumers of digital content and the perspective of children as creators of digital content.**

5. **The appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors online must:**

    a. **Include the ability of business users to clearly communicate different age requirements for consumers.** Platforms must provide traders with a way to communicate to their consumers if their applications are suitable for children from privacy and consumer protection perspectives in addition to content perspectives. The Commission guidelines must ensure that platforms allow their business users to follow European standards and regulatory requirements on the protection of minors.

    b. **Be based on clear responsibilities in the value chain.** Age assurance and verification, as well as GDPR consent management, should happen on the device level. Applications should always have access to age information from the parental control tools on the device level.

6. **The Commission should take a risk-based approach to age assurance and verification**. It should carefully evaluate when age assurance and verification processes are the appropriate solutions. Age assurance and age verification framework must not lead to situations where children's access to culture is limited due to regulatory burden or where parents' ability to control their children's digital environment becomes more limited. Furthermore, age assurance and age verification systems must not create market entry barriers.

2. In general

7. **The Commission should highlight the scope of the Digital Service Act (DSA) in the guidelines.** According to DSA:

    a. **Not all online platforms fall under the scope of DSA protection of minors obligations.**

        i. According to Article 3(i), an online platform is a *"hosting service that, at the request of a recipient of the service, stores and disseminates information to the public,* ***unless that activity is a minor and purely ancillary feature*** *of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation"*

        ii. According to Article 19, the "*Additional provisions applicable to providers of online platforms",* that DSA protection of minors requirements are part of, **do not apply to micro and small enterprises.**

    b. **Some protection of minors obligations under DSA only apply to very large online platforms.** These include, for example, the obligation to carry out risk assessments (Article 34) and the obligation to take targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate (article 35).

8. **The Commission should not push a one-size-fits-all approach through its guidelines.** Instead, it should acknowledge that different services, products and technologies require different approaches.

3. Balancing the fundamental rights

Table 1: Key fundamental rights		
UN CONVENTION ON THE RIGHTS OF THE CHILD		**EU CHARTER OF FUNDAMENTAL RIGHTS**
Rights protecting children	**Rights empowering children**	**Rights of the artistic creators**
Protection of minors from content not appropriate to their age (Article 31)	Right to leisure (Article 31)	Freedom of arts (Article 13)
Protection of children from inappropriate data practices (Article 16)	Right to participate freely in artistic and cultural life (Article 31)	Freedom to conduct business (Article 16)
Protection of minors and business models and unsuitable business practices (Article 36)	Right to actively participate in the (digital) community (Article 23)	
Right to protection from all forms of violence and exploitation (Articles 34 and 36)	Right to (digital) education (Article 28)	

9. **The Commission guidelines must be human rights-centric.** By principle, platforms should evaluate and balance all their policies on content and services allowed on their platforms from the perspective of fundamental rights and freedoms in the EU. This includes, for example, protection of minors from harmful content, protection from discrimination, right to privacy and securing their access to culture, as well as freedom of arts and expression, free movement of services on the digital single market area and freedom to conduct business. The same principle applies to the Commission while it is drafting the guidelines.

10. **In particular, the Commission guidelines must ensure the following.**

    a. **The guidelines must empower parents to take care of their responsibility for the upbringing and development of the child:** According to Article 18 of the UN Convention on the Rights of the Child, parents have the primary responsibility for the upbringing and development of the child. Therefore, the Commission must ensure that the guidelines ensure that parents, not platforms, have the primary control over, e.g., digital artistic content their children can access and their children's personal data.

    b. **The Commission guidelines must carefully ensure they respect children's right to leisure and participation in cultural life.** The Commission must carefully ensure that actions to protect children online do not lead to a situation where they start to limit children's access to digital culture that is suitable for their age. It is important to ensure that the protection of minors' practices does not just empower parents to make informed decisions; they must also empower children to make informed decisions in their digital lives. They must not just focus on risks of potential harm but also on empowering children to operate in the digital environment. E.g. access to PEGI content descriptors does not help just parents but also children to make informed decisions on the games they want to play.

    c. **The Commission must carefully balance all fundamental human rights while drafting the guidelines.** It is not enough for platforms to balance the fundamental rights in their decisions. As required by Article 3 of the United Nations Convention on the Rights of the Child, also the Commission must make the best interests of the child the primary consideration in all its actions. The Commission must carefully balance children's right to protection against their right to access culture. The Commission must carefully balance children's right to protection against the freedom of arts and the freedom to conduct business of digital content creators. Protection of minors should not be allowed to be used as an excuse to limit freedom of arts (e.g. by censoring content from adults) or limiting access to third-party mobile application stores enabled by the Digital Markets Act.

11. **The Commission should approach the protection of children from both the perspective of children as consumers of digital content and the perspective of children as creators of digital content.**

    a. **The Commission must ensure that the protection of minors' practices does not create unreasonable barriers for children to make their games and other digital content available to the public.**

    b. **The Commission must carefully evaluate what transparency obligations are truly necessary on platforms.** For example, it is crucial that there is a way for consumers to reach traders for support when needed. However, an email address is enough for this, and platforms should not force traders (who are minors) to publish their physical addresses on

the platform.

4. Clear responsibilities in the digital value chain

Table 2: European protection of minors framework		
Children rights	**Legal framework**	**Age ratings**
Protection of minors from content not appropriate to their age (e.g. explicit or violent content)	Co-regulatory PEGI system: PEGI Age Ratings and PEGI Code of Conduct	3, 7, 12, 16 and 18 years old
Protection of children from data practices not appropriate to their age	GDPR	The national age of consent varies between 13 and 16 years old, depending on the member state.
Protection of minors and business models and unsuitable business practices	European Consumer Law framework: protection of vulnerable consumers	Everyone under 18 years old is a vulnerable consumer
Right to protection from all forms of violence and exploitation	CSAM, Terroristic Content regulation	

12. **The appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors online must include the ability of business users to clearly communicate different age requirements for consumers:**

    a. **Platforms must provide a way for business users to communicate with their consumers if their applications are suitable for children from privacy and consumer protection perspectives in addition to content perspectives.** Currently, most digital platforms distributing digital games have an age rating system that communicates the suitability of the content of the digital games for minors. Unfortunately, these platforms do not provide a similar, easy way to communicate the suitability of their data processing practices and business models for children. In the worst case, the content of the game is ranked as suitable for children, while its business model is not, or its data processing practice requires parental consent. In the long run, the Commission should make efforts to fully harmonise all regulatory age restrictions based on PEGI age rating categories.

    b. **The Commission guidelines must ensure that platforms allow their business users to follow European standards and regulatory requirements on the protection of minors.** European co-regulatory pan-European PEGI and German USK age ratings are a vital part of pre-contractual information that must be communicated to players under European consumer law before they download a game. Furthermore, in some countries, their use is mandatory under national law. Unfortunately, some platforms (e.g. Apple) only allow the use of their own age ratings and do not allow the use of pan-European PEGI and German USK age ratings, and some platforms (e.g. Steam) do not use any age ratings at all. Consequently,

the Commission must ensure that platforms operating in Europe enable the use of co-regulatory pan-European PEGI and German USK age ratings for games.

Table 3: Responsibilities in the value chain

	Device/operating system level	Distribution platform level	Individual applications level
Examples	Microsoft OS, Apple iOS, Google Android	Apple Appstore, Google Play	Games
Relevant regulations	DMA, GDPR, Consumer protection, co-regulatory PEGI age ratings	DMA, DSA, GDPR, Consumer protection, co-regulatory PEGI age ratings, (CSAM), (Terroristic Content regulation)	(DSA), GDPR, Consumer protection, co-regulatory PEGI age ratings, (CSAM), (Terroristic Content regulation)
Examples of responsibilities	Operating system level protection of minors features: - Age assurance - Parental control tools and settings - Data management practices	Platform level protection of minors features: - Content moderation (on the distribution platform), - Transparency enabling informed consumer decisions	Application level protection of minors features: - Content moderation (if game is built on user-generated content), - Player support, - Safety by design, like modular game design, allows turning off features of the game that are not suitable for children - Community standards

13. **All gaming consoles, handheld devices and operating systems for PC and Mac are equipped with parental control systems[4].** These tools allow parents and caregivers to agree with their children, based on their age and maturity, what type of video game content can be accessed, whether in-game spending will be allowed or limited, or if any data may be shared with others online. Parents and caregivers are invited to set up accounts for their children. This provides parents with a significant degree of control over their children's online activities, including consenting to the processing of their children's data and managing with whom and how the child communicates and whether user-generated content may be shared.

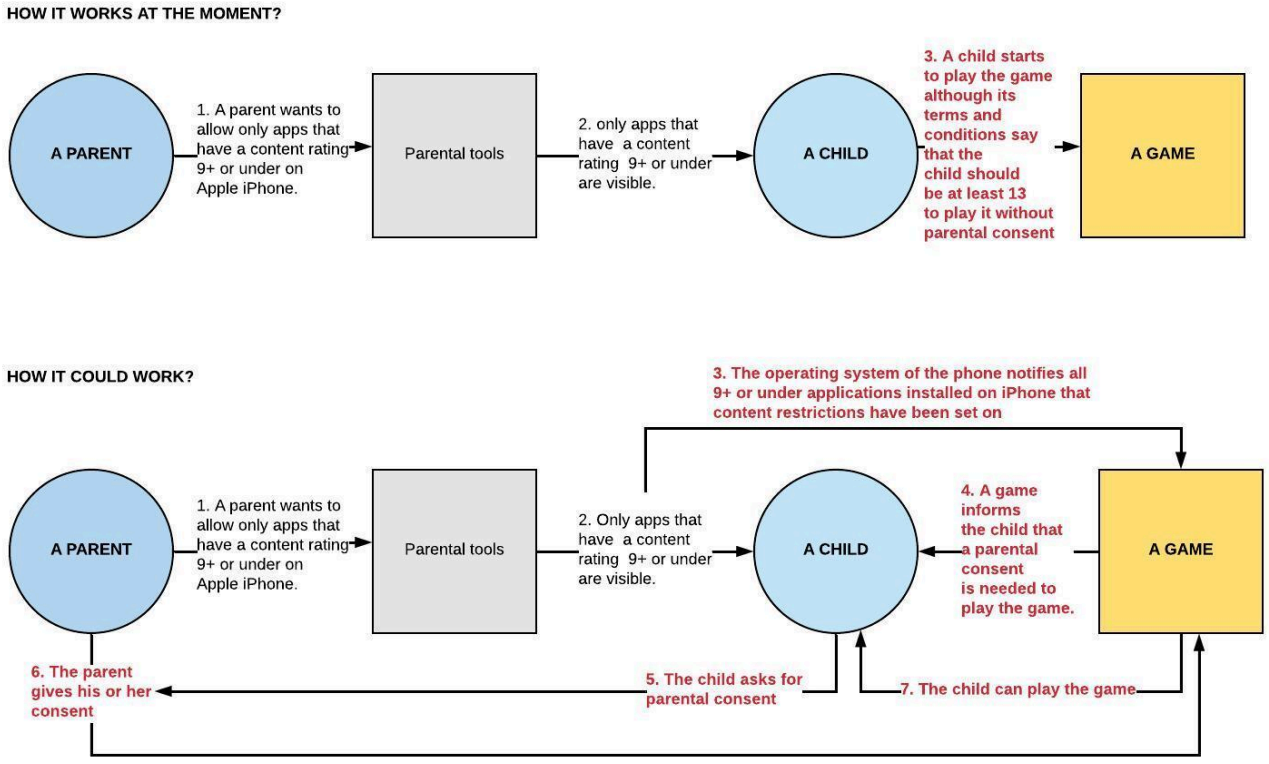
14. **The appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors online must be based on clear responsibilities in the value chain:**

[4] For more information, please visit: https://pegi.info/parental-controls

a. **When needed, age assurance and verification and GDPR consent management should happen on the device level.** Device-level centralised age verification solutions are the most privacy-friendly way to implement the age verification process, as end-users do not have to submit their age verification data separately to each service. Centralised age verification and parental consent management solutions are also the simplest for end-users to manage as they do not have to set them up separately for each application. They are also the best way to ensure trust in age assurance and verification solutions, as it would be highly challenging for parents and SMEs to fully evaluate the trustworthiness of different age verification and assurance service providers.

b. **Applications should always have access to age information from the parental control tools on the device level.** Currently, Google, for example, does not consider parental control tools to be core operating system services that it must provide access to under DMA. The Commission should ensure that in order to enable effective implementation of the protection of minor systems, both platforms and applications should have access to age information from the device-level parental control and consent management tools. See an example below on how the GDPR consent management should work.

c. **Clear protection of minors' responsibilities in the value chain removes important market access barriers for European SMEs.** Currently, there is a clear tendency, especially among mobile platforms, device manufacturers and operating systems, to push the protection of minors' responsibilities into the hands of game developers. Clear responsibilities (e.g. device level age assurance) for each party in the value chain make it easier for SMEs in the EU to launch their products. The absence of age assurance on the app level will help minimise the need to process children's personal data and optimise the app itself (device hardware resources will be redirected from age verification SDKs to app performance or new app features).



15. **The Commission must carefully evaluate when age assurance and verification processes are the appropriate solutions:**

    a. **The Commission should acknowledge that the protection of minors online can and should take many forms that should always be evaluated case by case** against the best interest of the child through internal risk-based analysis and assessment**.** Sometimes, this might include strict age verification; sometimes, a lighter age assurance should be enough, and in some cases, age verification or age assurance is not needed at all.

    b. **Age assurance and age verification frameworks must not lead to situations where children's access to culture is limited due to regulatory burdens.** If the protection of minors framework includes too much red tape and additional costs, it easily creates a situation where children are blocked by default.

    c. **Age assurance and age verification systems must not lead to a situation where parents' ability to control their children's digital environment becomes more limited.** The PEGI age rating system has been developed to help parents make informed decisions about the games their children play. Its purpose is not to block access of an 11-year-old child to PEGI 12-rated games. Its purpose is to ensure that the 11-year-old child must ask for parental consent to access PEGI 12 games. Mandatory age assurance and age verification processes easily create a systemic effect where the digital infrastructure no longer allows parents to adjust the digital environment to the level of maturity their child has reached.

    d. **Age assurance and age verification systems must not create a market entry barrier.** The EU digital identity wallet must be free for business users to use. Otherwise, access to it for age assurance and verification purposes easily creates a market access barrier.

    e. **Games are not played just in homes. Libraries, for example, are crucial actors in ensuring children's access to digital culture and overcoming the digital divide between socio-economic groups.** Age assurance and verification mechanisms should not be implemented in a way that they block or hinder the public use of VR devices, for example, when there is an actual human being checking the age of the player in the room.

    f. **Consequently, the Commission should take a risk-based approach to age assurance and verification.** The Commission should follow the national data protection authorities that have underlined in their guidelines that age assurance solutions should be proportionate to the identified risk, in particular when there is a potential impact on the fundamental rights of the user. A higher level of age assurance should only be required when the potential risks to the user are higher as well.

For more information, please contact:

Jari-Pekka Kaleva
Managing Director, EGDF
jari-pekka.kaleva@egdf.eu
www.egdf.eu