INTERACTIVE SOFTWARE
FEDERATION OF EUROPE
*Representing the European video games industry*

# ISFE Response to the ICO Public Consultation On Children and the GDPR

The Interactive Software Federation of Europe (ISFE) represents the European video games industry. Our membership comprises 16 major publishers and national trade associations in 17 countries throughout Europe. Our national associations in turn represent hundreds of games companies across Europe. Our industry is a world leader in driving new business models for the 21st century, and our annual contribution to the EU economy is now estimated at approximately €19 billion (Newzoo).

ISFE welcomes the opportunity to provide feedback on the Draft ICO Guidance on Children and the GDPR. We agree that fairness and compliance with the data protection principles should be central to all processing activities of children's personal data. The video game industry strongly supports the principle approach in the GDPR that children need particular protection when their personal data are collected and processed because they may be less aware of the risks involved. We have, therefore, undertaken a number of efforts to promote parental involvement, to protect children's privacy and to create a safer off and online environment for children.

In 2003, the video game industry established the PEGI system which operates through a set of scientifically backed ethical standards in the form of a Code of Conduct. The PEGI system is part of the industry's commitment to protect minors and behave responsibly where children are concerned. Each publisher that joins PEGI has to sign a Code of Conduct committing him/her to provide parents with objective, intelligible and reliable information regarding the suitability of a game's content. By signing the Code, the publisher also undertakes to maintain a responsible advertising policy, provide opportunities for consumer redress and adhere to stringent standards for a safe online gaming environment, such as the need to maintain an effective and coherent privacy policy which must encompass the responsible collection, distribution, correction, and security of the personal details of users. Such users must be given the opportunity to comment on any perceived misuse of their personal details and therefore be fully advised as to ways, for example, of avoiding unsolicited or unwanted e-mail contact[1].

The PEGI system is recognised by the European Commission and considered as a model of European harmonisation in the field of minor protection and consumer transparency. It is overseen by a number of independent bodies such as the PEGI Council with officially designated representatives of the European Member States and Institutions, the PEGI Experts Group is comprised of specialists and academics in the fields of media, child psychology, classification & technology, and the PEGI Complaints Board and Enforcement Committee composed of independent experts. The content ratings themselves are given by designated independent games rating authorities who review and monitor all declarations by PEGI signatories.

In 2013, the video game industry established IARC, The International Age Rating Coalition, which comprises rating boards from Europe, North America, Brazil and Australia who have joined

[1] Article 9.4 of the PEGI Code

forces to provide a solution for the globalised market of apps. IARC informs the consumer about certain types of functionality in an app, such as in-app purchases, location data sharing, unrestricted internet access and the ability of users to interact. In terms of participating storefronts, IARC has now been adopted by Mozilla Firefox Marketplace, Google Play Store, Microsoft Windows Store, Nintendo® eShop and the Sony PlayStation® Store. The participating rating authorities collectively represent regions serving approximately 1.5 billion people.

The video game industry's robust parental control tools are the most sophisticated available among all entertainment media. These not only allow parents to control access to video game content based on their child's age and maturity but also allow parents to manage and control how their children access the internet, share their data and interact with others online. Parents can set up accounts for their children providing them with a significant degree of control over their children's online activities, including managing with who and how the child communicates and whether user-generated content can be shared.

Our sector has indeed always been extremely vigilant in protecting the interests of children when designing new products and systems. The Guidance unfortunately does not always provide sufficient clarification on how to implement the new rules in this respect.

We are concerned that the lack of clarification in the Guidance would create regulatory uncertainty which may impede the ability of video game publishers to maintain the range of online entertainment options available to children. ISFE therefore urges the ICO to provide clarification or revise the proposed Guidelines in the following key areas so that operators can continue to innovate and offer interactive online experiences to children in ways that meaningfully protect their privacy and security.

**How to deal with audiences that include a wide variety of age ranges?**

The guidelines recommend taking a cautious approach if a controller isn't sure whether the data subjects are children, or what age range they fall into. It is then further explained that such a cautious approach could include designing the processing of data to provide sufficient protection for children, putting in place proportionate measures to prevent or deter children from providing their personal data and taking appropriate actions to enforce any age restrictions you have set or implementing up-front age verification systems. The choice of solutions may vary depending upon the risks inherent in the processing, the rights and freedoms of the child, and the particular provisions of the GDPR that apply to your processing.

Video games are consumed by a wide variety of consumers of all ages[2]. Age classifications provide for a minimum age for which a given product is considered suitable, but they do not provide information on whether the game can be played by this particular age group, nor whether this group constitutes the "target audience" of the game. A chess game, for instance, will always be classified as suitable for all ages, although very young children will find it too difficult to play.

[2] The latest statistics can be found on the ISFE website.

The general recommendation that proportionate measures must be applied when it is unsure whether children are part of the audience may easily slip into disproportionate requirements on video game publishers such as the need to apply strict measures or age verification tools, even where the publisher has set age limits on accounts and has no actual knowledge that any children are playing its game or – if age verification is not feasible or not to be applied in the interest of data minimization – to treat *all* their users as children. This is particularly true as for the purpose of this Guidance children are defined as under the age of 18. This guidance goes beyond the GDPR, which does not require that children are defined as under 18 and goes beyond existing practice in the UK that a child, for the purposes of the 1998 Data Protection Act, is anyone under the age of 13. Current ICO guidance[3] states the following:

> There are many difficulties when collecting information from children, including determining whether parental consent to data collection should be obtained and, if so, what form it should take. For example:
>
> - In the UK there is no simple legal definition of a child based on age. Even if there was, you might not know the ages of many of the individuals you are dealing with or be able to rely on the information provided by the child or "adult" as to age.
> - Children of a similar age can have different levels of maturity and understanding. Consideration of these attributes, as well as age, will be required to ensure that children's data is processed fairly.
> - A resourceful and determined child could circumvent many mechanisms for obtaining his or her parent's consent for the collection of personal data.

We believe this continues to be a more sensible approach and would still be compliant with GDPR. There is no need to state that 'children' must always be interpreted as under 18 when flexibility has been shown to work in the existing system.

In relation to the issue of whether a service is actively targeting UK children, we believe that it would be imperative for the ICO to establish, in consultation with the industry, objectively fair criteria to determine whether a service is "actively" targeting UK children. Does offering a service in the English language play a role in such an assessment? Online storefronts, for instance, often have no national establishment but are offering products and services to consumers from different countries, sometimes outside Europe. What happens when an American or Irish website also serves British consumers? We ask for further clarification on this important point.

**How to make reasonable efforts to verify whether anyone giving consent is old enough to do so or holds parental responsibility?**

The Guidance fails to sufficiently explain and illustrate examples of what can be considered as reasonable age verification methods in both high-risk as well as low-risk processing situations. The Guidance states that "The Commissioner believes that there are suitable technologies in the marketplace, but she is not in a position to provide recommended services at the present time." It is unclear why this is the case. Is this because technological solutions, such as biometric and

[3] The Personal Information Online Code of Practice, available at https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf

age verification systems can easily be circumvented and vary heavily in terms of the level of assurance they offer? If there is not a single system that offers sufficient assurance to be applied as a one size fits all solution on a national basis then that should be stated clearly. We ask for clarity whether any examples exist of what might be considered appropriate methods for obtaining and verifying parental consent.

The Guidance recommends using "a third-party verification service - to verify that the child is old enough to provide their own consent". Again, concrete examples of such a service in the UK would be welcome. It is questionable whether such services would be able to operate legally in the UK. They would have to process the date of birth and contact information for the child as this increases the amount of personal data that is processed about the child, and potentially also the processing risk. In addition, the videogames industry is essentially an international business so that solutions that may work only in individual countries do not seem feasible.

**How to assess children's competences to agree a contract?**

The Guidance correctly states that consent is not the only basis for processing children's personal data in the context of an information society service. It further says that if a company wishes to rely upon 'performance of a contract' as a lawful basis for processing, the child's competence to agree to the contract and to understand the implications of this processing must be considered. The Guidance however does not explain how such an assessment should be done and generally refers to external legal advice regarding the "complex area" of entering into contract with a minor. Companies might not always have the financial means to get external legal advice and it unfairly imposes the risk of such external legal advice being agreed with later by supervisory authorities solely on companies. More detailed guidance is needed on the use of the contractual legal basis in relation to the processing of children's data. Contracts that can be easily voided may render the processing unlawful and create substantial legal uncertainty which will have an impact on the industry's competitiveness and growth.

The Guidance further notes that parents can only exercise the data protection rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evidently in the best interests of the child to do so. It is again unclear how such an assessment can be made as even children of the same age can have very different literacy levels.

**How to apply the right to information to a children's audience?**

The Guidance notes that privacy information directed to children should always be age-appropriate and, as far as possible, addressed directly to the relevant age group. This industry has vast experience of communicating with consumers of all ages and has created many different innovative ways to inform consumers, for instance by using icons to provide appropriate information and advice regarding the content, functionality and age suitability of a product. While we strongly support the GDPR's transparency obligations to always use language that is sufficiently concise, clear and accessible we want to caution that there is no single language that can be equally plain and clear for all the various age and user groups.

The Guidance also recommends providing different versions of the privacy notice if the target audience covers a wide age range, even in cases where parental consent is triggered as the lawful basis. It is our understanding however that in cases where Article 8 applies the privacy notice must be directed to the holder of parental responsibility. It should be clarified that this suggestion should be considered as good practice that will help raise the level of protection to children and that it is not mandatory under the GDPR.

ISFE Secretariat, February 2018