Fundamentals for a Child-Oriented Approach to Data Processing
ISFE EGDF response

Key Recommendations

- ISFE and EGDF recommend that the main criterion for assessing whether organisations need to comply with the standards and expectations of the Fundamentals should be whether the services they provide are directed at or intended for children.
- ISFE and EGDF recommend clarifying the steps that need to be taken to ensure that age verification mechanisms are effective when a service provider stipulates that its service is not for the use of children below a certain age.
- ISFE and EGDF recommend that the Fundamentals take into consideration that it is not always possible for organisations to offer services without any type of consent-based data collection.
- ISFE and EGDF recommend the DPC to reconsider its position that marketing and advertising activities in pursuit of commercial/business interests of an organisation will generally not align with its "zero interference with the best interests of the child" principle.
- ISFE and EGDF recommend that the Fundamentals recognise the central role that parents and legal guardians can play in helping their children understand the risks of data processing activities and ensuring that they have the benefit of specific protection under the GDPR.

Introduction

1. ISFE and EGDF welcome the opportunity to provide feedback on the Draft Fundamentals for a Child-Oriented Approach to Data Processing. We strongly support their overall objective of enhancing the level of protection afforded to children and providing assistance to organisations by clarifying the principles arising from the high-level obligations under the GDPR. As an industry, we are very committed to the GDPR's principal approach that children need particular protection when their personal data is collected and processed because they may be less aware of the risks, consequences and safeguards concerned.

2. The video games industry is aware of the risks related to children in digital environments and understands the importance of establishing practical measures and safeguards. Our sector has undertaken a number of initiatives, which are summarised below, that go beyond mere compliance with the law and set self-regulatory standards to protect children's privacy, create a safer off- and online environment and promote the involvement of parents and carers.

INTERACTIVE SOFTWARE FEDERATION OF EUROPE aisbl.
Rue Guimard 15 | 1040 Brussels | Belgium
T +32 2 612 17 78 | info@isfe.euinfo | www.isfe.eu

3. These standards demonstrate our commitment to respect the rights of the child and those of the parents. They also demonstrate how we always place the best interests of the child as a primary consideration when products and services are being developed, as was envisaged by Article 3 of the United Nations Convention on the Rights of the Child.

Self-Regulatory Standards and Responsible Practices

4. 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[1]. The PEGI system is part of the industry's commitment to protect minors and to behave responsibly where children are concerned. Each publisher that joins PEGI has to sign a Code of Conduct committing it 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, maintain community standards and adhere to stringent standards for a safe online gaming environment. These include 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 who 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[2].

5. 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 EU Member States and Institutions, the PEGI Experts Group which is comprised of specialists and academics in the fields of media, child psychology, classification and 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 Ireland, games with a PEGI rating are exempt from mandatory classification by the Irish Film Classification Office which represents the country in the PEGI Council.

6. In 2013, the industry established IARC, The International Age Rating Coalition, which comprises rating boards from Europe, North America, Brazil and Australia who have joined forces to provide a solution for the globalised market of apps, collectively representing regions serving approximately 1.5 billion people. IARC has now been adopted by Google Play Store, Microsoft Windows Store, Nintendo® eShop and the Sony PlayStation® Store, and 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. This gives users, including parents, further information about

[1] https://pegi.info/pegi-code-of-conduct
[2] Article 9.4 of the PEGI Code

games and other apps, in addition to the age rating and content descriptors provided by the games age rating bodies.

7. The PEGI classifications are supported by sophisticated and robust parental control tools[3] on a variety of devices and software applications that not only allow parents to control access to video game content based on their child's age and maturity but also provide them with a significant degree of control over their children's online activities. Parents can set up accounts for their children to allow them to manage and control how long they can play, how much they can spend, if and how they can interact with others online, and whether personal data, such as user-generated content, can be shared.

8. Most of the 14 Fundamentals that have been identified by the Data Protection Commission (DPC) fully underpin the work we have been doing so far. For some of them, however, implementation is not always clear cut. We are concerned that some aspects of the guidance on how these Fundamentals should be implemented in practice may be ambiguous or may even have a contrary effect on the protection of children's privacy. We will highlight these concerns below.

The Scope: Providing a Floor of Protection or Verifying the Age

9. The DPC considers that organisations should comply with the standards and expectations established in these Fundamentals when the services provided by the organisation are *directed at, intended for or likely to be accessed by children*. "Likely to be accessed by children" is simply explained as "more likely than not", while children are defined as persons under the age of 18.

10. Online service providers should provide a "floor" of protection for all users unless they take a risk-based approach to verifying the age of their users so that the protections are applied to all processing of children's data. The Fundamentals therefore require that organisations "know" their users and have knowledge about the people they collect information on. It is suggested that this may be done through conducting user testing, market research, user consultation and artificial intelligence. Furthermore, a reference is made to a non-exhaustive list of factors that have been identified by the US Federal Trade Commission (FTC) in its role as regulator for enforcing the US Children's Online Privacy Protection Act (COPPA), for the purposes of assisting operators in analysing who their intended, actual or likely audience is.

11. Market research and user testing is however very costly and difficult to execute in the context of a children's audience, as retrieving such information from children requires parental consent and oversight. It is questionable whether the use of artificial intelligence can provide reliable information about the age range of children who are "*likely to access"* a service in the context of video games. While the FTC's list of factors may certainly be helpful in such an assessment, it does not allow the establishment with

[3] Information about the functioning of these tools can be found here: https://pegi.info/parental-controls

a sufficient level of certainty of the probability that a certain age range of children is accessing a service.

12. ISFE and EGDF are concerned that the lack of a robust methodology to identify beyond any doubt the age ranges of the children who access a service will create uncertainty for video games publishers about the level of protection that they need to apply on their services. Age classification cannot be of any help in this respect either. While video games are consumed by a wide variety of consumers of all ages, age classifications only provide for a minimum age for which a given product is considered suitable and not for information on whether the game can be played by this particular age group, nor whether this group is "likely" to access 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.

13. Any online service with underaged users will effectively face the choice of applying by default the highest level of privacy protections to all users (including adult ones) or of using an age verification method to exclude children completely. The latter will be the most economically viable option for services with a mixed audience. Uncertainty about the age of the users likely accessing their services will push service providers to exclude their underaged audiences. This may result in child users circumventing age verification measures or accessing services with content not intended for their age. It may also result in service providers inadvertently falling foul of Fundamental 10.

14. ISFE and EGDF therefore recommend that the main criterion for assessing whether organisations need to comply with the standards and expectations of the Fundamentals is whether the services they provide are directed at or intended for children.

Exercising children's data protection rights

15. ISFE and EGDF agree with the DPC that age alone is not a good metric for assessing the capacity of a child to exercise his or her data protection rights as there can be considerable variation in cognitive development in children of the same age, particularly in early adolescence. The assessment of whether a child has the developmental capacity to understand the safety and privacy issues that can result from the online collection of personally identifiable information and whether the context of a data processing activity would allow him or her to exercise his or her own data protection rights, should be done by those who best know the child: the child's parents or legal guardians. The Convention of the Rights of the Child clearly recognises the responsibilities, rights and duties of parents or legal guardians who have a primary responsibility for the upbringing and development of the child and must ensure its best interests. It obliges them to provide guidance in the exercise of the child's rights in a manner consistent with the evolving capacities of the child.

16. Such an approach requires parents and legal guardians to establish a dialogue with the child about the importance of these rights and the implications of using them. Our industry understands the importance of such conversations and actively encourages

parents/legal guardians to accompany their children when experiencing video games. We believe that a direct child-parent interaction is essential to provide the necessary guidance in the exercise of children's data protection rights. This is particularly the case for younger children or those that are not at developmental capacity, where they will rely on their parents/legal guardians to help them understand and exercise such rights on their behalf. Our sector has therefore conducted several public awareness campaigns to inform parents on how to start a dialogue and take an interest in their children's online activities. Where parents or legal guardians consider it necessary to act on behalf of and in the best interests of the child, our industry's parental control tools will be at their disposal.

The age of consent and age verification

17. Age verification efforts can be undertaken by organisations for different purposes which should be distinguished. Article 8 of the GDPR requires organisations to make "reasonable efforts" to verify – where a child is below the age of consent – that consent is given or authorised by the holder of parental responsibility over the child. This implies that a form of (age) verification needs to take place. The guidelines of the European Data Protection Board (EDPB) make clear that it is up to the data controller to determine what measures are appropriate in a specific case. As a general rule, verification solutions which themselves involve excessive collection of personal data should be avoided to comply with GDPR's data minimisation principle. The EDPB however fully acknowledges that verification can be challenging, and that this should be taken into account when deciding what is reasonable.[4]

18. Our industry's parental control tools allow parents or legal guardians to set up accounts for their children enabling them to give or withhold consent to the processing of their children's data. Such a framework establishes a direct relationship with parents and legal guardians as users in their own rights of an account-based service and offers an easy route to verifying parental consent while limiting the need for additional data collection from the child. This approach, which is recommended in the Fundamentals, allows organisations to easily verify consent without excessive collection of personal data. Parents or legal guardians have access to a functional dashboard or settings where they can always re-confirm, modify, or withdraw their consent.

19. The Fundamentals state that the requirements around the age of digital consent should not impose restrictions on a child being able to access a service and that data protection compliance can in no way justify the "locking-out" of children from a rich user experience, as this would deprive children of their full rights under the UN Convention of the Rights of the Child. While it is important to protect children's rights to play and access, it is not always possible that video games companies can provide all features of a game experience to underage players without obtaining parental consent. For instance, some game features may include social, communications or content sharing features that may require verified parental consent for underage users. Games platforms or publishers often provide mechanisms for parents to provide consent for their child's

[4] EDPB Guidelines 05/20 on consent, p. 29.

participation in these features. Where that consent isn't possible, games companies may disable those features for younger users. These features are often ancillary to gameplay and underage players still enjoy a rich user experience.

20. ISFE and EGDF agree with the DPC that the methods to establish or verify age should be proportionate and grounded on a risk-based approach whereby greater levels of assurance should be proportionate to the risk arising from the data processing. We also welcome the DPC's acknowledgement that self-declaration may be suitable for low-risk processing situations. However, where a service provider stipulates that its service is not for the use of children below a certain age, the DPC requires that it take steps to ensure that its age verification mechanisms are effective at preventing children below that age from accessing its service. The Fundamentals do not explain which practical steps organisations should take to prevent this from happening. Nor do they indicate which mechanisms would be sufficiently robust to provide a high level of certainty about the age of a child in more risky processing situations. Practical guidance as to what services are deemed more likely to be high risk processing situations to various ages of children would assist organisations assess how they can best fulfil the requirements.

21. When parents or legal guardians set up accounts for their children offering parental control systems, they must confirm the age of the child. Such an approach already provides a high level of assurance to verifying the age of the user. All video game consoles, for instance, provide parental control systems and allow games to access information on whether or not those systems are activated. Any additional solution should be able to enhance the level of assurance of the verification process. Furthermore, such a solution should also be cost-effective, implementable in different technical environments, and applicable to users across global borders and as frictionless as possible to meet the expectations of what users. It is questionable whether such a solution currently exists. Age verification systems face numerous technical and legal obstacles to function efficiently and vary widely in terms of the level of assurance they offer.

22. ISFE and EGDF recommend clarifying the steps that need to be taken to ensure that age verification mechanisms are effective when a service provider stipulates that its service is not for the use of children below a certain age. Furthermore, the Fundamentals should also take into consideration that it is not always possible for organisations to offer services without any type of consent-based data collection.

Direct Marketing, Profiling and Advertising

23. ISFE and EGDF welcome the DPC's acknowledgement that contextual advertising on child-focused online services which deliver advertisements based on on-screen content is beyond the scope of data protection law. Direct marketing, defined as any activity attempting to promote a product or service by targeting an individual, is on the other hand very much in scope and the Fundamentals argue that such marketing to children would only be permitted in limited circumstances.

24. Where direct marketing is carried out through the sending of electronic communications directly to the user, it is subject to ePrivacy law. Such marketing would require consent as a legal basis unless the contact details of the consumer were obtained by the marketeer as a result of a sale. Other forms of marketing are subject to the GDPR and may be regarded as carried out for a legitimate interest which is explicitly recognised in Recital 47. Invoking legitimate interests as a legal basis under the GDPR requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights and freedoms of the data subject whereby particular emphasis is placed on the need to protect children. This is recognised in Recital 38 of the GDPR which says that children require specific protection with regard to their personal data because they may be less aware of the risks and consequences of the processing.

25. The Fundamentals however argue that in cases where organisations are processing children's personal data on a legitimate interest basis the balancing test needs to be *recalibrated* whereby these organisations need to ensure that the legitimate interests pursued do not *interfere with,* conflict with or negatively impact, at any level, the best interests of the child. This forms the basis of the DPC position that marketing and advertising activities in pursuit of commercial/business interests of an organisation will generally not align with such a "zero interference with the best interests of the child" principle.

26. While there is no outright prohibition on conducting direct marketing activities towards children, we agree that the principle of the best interests of the child should remain a key criterion in assessing whether the conduct of such activities is in line with the principles concerning the special protection of children under the GDPR. However, the purpose of the balancing test is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent a disproportionate impact on the data subject. This is a crucial difference. The emphasis on protecting children does not prohibit the use of this legal basis but merely requires the controller to consider a higher threshold regarding the data protection risks and the measures needed to contain them[5]. Furthermore, as recognised in the Irish Code of Standards for Advertising and Marketing Communications, the way in which children perceive and react to marketing communications is influenced by their age, experience, and the context in which the message is delivered[6]. A controller therefore needs to consider that the age and maturity of the child may affect the balance as well whereby older children are less likely to be disproportionately impacted.

27. We therefore cannot agree with the DPC's position that an organisation's legitimate interest will always be overridden when data of any child under the age of 18 is processed for the purpose of advertising, as the organisation may be able to demonstrate that, taking account of the child's age and maturity, and the context of the advertisement, such processing has a minimal or no effect at all on the interests or fundamental rights and freedoms of the child or that it can even be mutually beneficial

[5] -Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Article 29 Working Party, p. 41
[6] - Code of Standards for Advertising and Marketing Communications in Ireland, Art 7.3.

for both parties. Advertising to children is, for instance, bound by strict rules which are rigorously enforced by Advertising Standards Authorities around the world, while the emergence of new industry standards such as the Transparency and Consent Framework[7] allow users to freely choose whether to receive such marketing or not. Advertising to children has also helped create a diverse and vibrant market for children's products which sparks creativity, imagination and curiosity.

28. Finally, we also want to highlight that profiling can be used to serve a wide range of other purposes beyond advertising and marketing. In our industry, these include fixing areas of a game that prove problematic to progression, identifying fraud, remembering content that was recently played, providing hints to the player, creating scoreboards or personalising gameplay settings. All these processing activities enable or improve the gameplay experience and have aligned very well with the best interests of the child and do not negatively impact their fundamental rights and freedoms.

29. ISFE and EGDF recommend the DPC to reconsider its position that marketing and advertising activities in pursuit of commercial/business interests of an organisation will generally not align with its "zero interference with the best interests of the child" principle. Data processing for the purpose of advertising can have a minimal or no effect at all on the interests or fundamental rights and freedoms of the child or even be mutually beneficial for both parties.

Tools to ensure a high level of data protection for children.

30. Even before the GDPR entered into force, the industry adopted Privacy by Design as a key design principle when new products and systems are being developed. Gameplay data, for instance, are often collected and stored in a way that does not allow companies to identify the player directly by applying technical and organisational measures to prevent easy linking between the gameplay dataset and the players' account information. Companies also try to minimise the collection of personal data to what is needed for each processing purpose and have long since endorsed the use of pseudonymised data as a valid way to protect the identity of underaged users. Pseudonymised datasets are much safer to handle but still allow the personalisation of the user experience.

31. We believe that a direct child-parent interaction is also essential to ensure that children enjoy the best possible protection. Our approach to implementing solutions is guided by the principle of active choice: we have found that it is more effective to ask parents or legal guardians to make a series of choices as to the level of parental control and filtering on a device, making them mentally engage with what is appropriate for their family, than to simply have all such controls switched on automatically when they first use the device. Applying by default the highest privacy settings, switching off all geo-localisation by default or displaying an online sign when a parental supervision system is activated cannot substitute a proper face-to-face conversation. It is much more effective to engage with children and explain in which context a certain feature can be risky and should be

[7] - See: https://iabeurope.eu/transparency-consent-framework

avoided. Furthermore, the requirement that a default privacy setting that has been turned off by the child, should automatically be switched on again at the end of a session, would go against the position in Fundamental 7 that children should be able to exercise their own data protection rights if they have the capacity to do so and it's in their best interests.

32. It is important to differentiate between exact geolocation data and general geolocation data. The first one, often based on GPS data, is already required to be automatically turned off on leading mobile platforms. The second one, however, is needed for determining the country of the player to apply the appropriate consumer protection rules and correct VAT rate. General geolocation data are also used to combat fraudulent online activities, tackle toxic or criminal online behaviour, and keep children safe online. They are an important tool for ensuring that an online service is safe and secure which is why they are often activated by default. This should be counter-balanced against the potential misuse of such data or the perceived loss of privacy.

33. An effective engagement with children about potential risks of data processing activities can only happen if parents or legal guardians are well informed. Our sector has a track record of communicating to parents, care givers and players to promote the use of parental controls whereby we take great care to emphasize that these tools are best utilised by parents, legal guardians and children working together to understand games and gameplay, rules and boundaries.

34. ISFE and EGDF therefore recommend that the Fundamentals recognise the central role that parents and legal guardians can and must play in helping their children understand the risks of data processing activities and in ensuring that they have the benefit of specific protection under the GDPR.

ISFE and EGDF Secretariats, March 2021

About ISFE

1. ISFE represents the video games industry in Europe and is based in Brussels, Belgium. Our membership comprises of national trade associations in 15 countries across Europe which represent in turn thousands of developers and publishers in the Member States. ISFE also has as direct members the leading console manufacturers and European and international video game companies, many of which have studios with a strong European footprint. They produce and publish interactive entertainment and educational software for use on personal computers, games consoles, portable devices, mobile phones and tablets.

2. ISFE's purpose is to serve Europe's video games ecosystem by ensuring that the value of games is widely understood and to promote growth, skills, and innovation policies that are vital to strengthen the video games sector's contribution to Europe's digital future.

The video games sector represents one of Europe's most compelling economic success stories. Relying on a strong IP framework, the sector is a rapidly growing segment of the creative industries. In 2019, the size of Europe's video games industry was €21 billion and it registered a growth rate of 55% over the past 5 years in key European markets[8].

3. Video games have a proven ability to successfully drive new business models. The digital transformation with the growth of online and app-based gaming represents today 76% of the industry's total European revenues. Via the launch of new high-performance consoles and the strong growth of mobile gaming, the industry offers players across Europe and in all age groups the possibility to enjoy and engage with video games[9]. Today, 51% of Europe's population plays video games, which is approximately 250 million people, and 54% of the players regularly play on consoles.

About EGDF

1. The European Games Developer Federation e.f. (EGDF) unites national trade associations representing game developer studios based 19 European countries: Austria (PGDA), Belgium (FLEGA), Czechia (GDACZ), Denmark (Producentforeningen), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Malta (MVGSA), Netherlands (DGA), Norway (Produsentforeningen), Poland (PGA), Romania (RGDA), Serbia (SGA), Spain (DEV), Sweden (Spelplan-ASGD), Slovakia (SGDA), Turkey (TOGED) and the United Kingdom (TIGA). Altogether, through its members, EGDF represents more than 2 500 game developer studios, most of them SMEs, employing more than 35 000 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. European digital single market area is the third-largest market for video games globally. All in all, there are around 5000 game developer studios and publishers in Europe, employing closer to 80 000 people.

3. Good user experience is vital for the success of the game developer studios. For this reason, game developers follow the best accessibility, data protection, protection of minors and consumer protection practices. Video games companies collect data to improve the game experience, identify bugs, fight toxic online behavior, identify security threats, identify business frauds and to improve their business models.

[8] ISFE Key Facts 2020 from GameTrack Data by Ipsos MORI and commissioned by ISFE
[9] See also https://www.isfe.eu/data-key-facts/