Information Commissioner’s Office Consultation: Age Appropriate Design Code

Response from Ukie, the Association for UK Interactive Entertainment

Contact: [redacted] **Tim Scott, Head of Policy and Public Affairs**

Contents

Executive summary

1. Whilst putting the best interests of the child at the heart of any Information Society Service ("ISS") design is a worthy ambition, we are greatly concerned about the practical implementation and implications of the proposed scope of the code. Treating all services that could ever be accessed by a child as in scope is too broad a definition and may lead to an unworkable Age Appropriate Design code ("Code").

2. There has been a lack of meaningful consultation leading to a lack of clear evidence to justify these measures. This far reaching code needs more engagement and consultation in order for it to be appropriate, proportional and effective.

3. The code goes beyond GDPR requirements, extending into content regulation and requiring further significant investment by companies in order to achieve compliance which would be better invested in further safeguarding measures.

4. The means of complying with the code are not cost-effective especially in conjunction with the short implementation period. Requiring different age appropriate versions of a service according to a user's age group, and/or the use of "robust" age verification, can increase costs for both a business and the consumer.

5. Age-verification is fraught with problems and would lead to data maximisation, not minimisation. Employing a third party to undertake the age verification on an ISS' behalf, to the extent such services even exist and are scalable, would be costly, add greater risk to data protection and be open to legal challenge.

Key Recommendations

6. Clarify the scope of the code by giving further detail on what *'likely to be accessed by a child'* means, with reference to previous regulatory examples.

7. Adopt a more proportionate, risk-based approach where only services clearly targeted at children under the age of consent are within the scope of the code and ensure that the code fully reflects the UK's obligations under the UN Convention on the Rights of the Child, balancing the right to privacy against the other rights included.

8. Undertake further work after this consultation period assessing the full impact of the code, such as a formal economic impact assessment but also practical workshops with a wide range of companies - including game publishers and developers - to map out the practical impact that different ISS providers will face.

9. Undertake a technical feasibility study on age verification mechanisms to ensure that companies where in scope would be able to comply with the code.

10. Subject to the foregoing, allow for the maximum implementation period when the code comes into force, to ensure ISS providers have time to adapt to the code.

About us

11. Ukie is the trade body for the UK's games and interactive entertainment industry. A not-for-profit, it represents more than 450 games businesses of all sizes from start-ups to multinational developers, publishers and service companies, working across online, mobile, console, PC, esports, virtual reality and augmented reality. Ukie aims to support, grow and promote member businesses and the wider UK games and interactive entertainment industry by optimising the economic, cultural, political and social environment needed for businesses to thrive.

12. Ukie welcomes the opportunity to respond to this consultation on the draft. Our response reflects the fact that our industry considers the safety of our player community as paramount. With over 2 billion players, it's paramount to our industry to create a safe environment and provide information and tools to allow parents and carers and players to safely enjoy their experience.

The Games Industry

13. Our response reflects the fact that our industry considers the safety and interests of our player community as paramount. Our industry has a player first approach. With over 2 billion players, it's paramount to our industry to create a safe environment and provide information and tools to allow parents, carers and players to enjoy a safe, fun, fair and inclusive playing experience.

14. Our sector has a strong track-record in self-regulation and has been at the forefront of technological innovation for many years.

Age Ratings

15. The Pan-European Games Information, (PEGI) is the sole system used for new console and PC games. PEGI is used and recognised throughout Europe and is supported by the European Commission. Many thousands of games have been PEGI-rated since the scheme was devised and introduced in early 2003. It is important to note that in the UK, PEGI 12, 16 and 18 ratings are legally enforceable meaning that they cannot be supplied to persons below those respective age bars. There are also strict measures by the emerging esports industry in the UK to ensure that games cannot be viewed by anyone under the age rating for the game. The body responsible for applying UK PEGI ratings is the Video Standards Council (VSC).

16. 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.

17. It is important to note, that the PEGI rating on a game confirms that it contains content suitable for a certain age group and above. So a 7-rated game is suitable for everyone who is seven or older, while an 18-rated game is deemed suitable for adults only. It is not, however, a measure of who will enjoy the game or how difficult that game is.

18. Outside of PEGI, the Apple App Store is the largest markeptplace for mobile content. The App Store also has its own rating and categorisation system. Each app has a recommended age, ranging from 4+ to 17+. Those which are rated the later are prohibited from purchase by younger users. Furthermore, the App Store include a 'Kids' section for child-appropriate apps. Apps and games follow a stringent process in order to be accepted onto the 'Kids' section by complying with the appropriate guidelines.

Impact

19. We are concerned that the code's impact on current internet and online services will be drastic and that the extremely narrow timeframe for consultation on such far reaching proposals, coupled with concurrent prospective pieces of legislation, such the Online Harms White Paper proposals, risks undermining the positive intention of the code. This is an extremely complex area of policy which merits additional time, care and extensive consultation and collaboration. Further, as Section 125 of the Data Protection Act 2018 ("***Act***") only requires the Information Commissioner to submit the code to the Secretary of State for approval within 18 months of the passing of the Act (i.e. by 23rd November 2019), we do not understand the rationale for the extremely short consultation period.

20. We are not aware of any other country interpreting GDPR so strictly. The cost of compliance will be high for businesses of all sizes.. For many global services, the simplest and most effective response will be to simply limit or stop prioritising UK audiences [1]. Furthermore, We fear it will be the specifically UK companies who will be worst hit, damaging the UK's reputation as a world leader in these innovative and ambitious sectors, just when we need to be leading the way globally.

21. We therefore recommend that further work is undertaken following this consultation period to assess the full impact of the code; for example, by initiating a formal economic impact

[1] The UK is the 6th largest video game consumer market valued at £5.7bn http://ukie.org.uk/research#Market

assessment, as well as practical workshops with a wide range of companies – including e-commerce platforms, games publishers and developers – to map out the practical impact that different ISS providers will face.

Scope

22. The code takes a very broad interpretation of what "*likely to be accessed by children*" means, which also conflicts with related legislation on what constitutes the age of a child. For example, the code requires ISS providers to consider that all users under 18 are children while the provisions of the CAP Code [2]and relevant guidance clearly define children as being under 16 and only apply the CAP Code to marketing communications "*addressed to, targeted directly at or featuring children*", a higher standard than the code.

Member Quote: "by requiring us to assume that all users are children unless we know otherwise, this Code would require many online businesses to implement all the provisions of the CAP Code and relevant guidance, even though the CAP provisions only apply to marketing communications "addressed to, targeted directly at or featuring children", a higher standard than the ICO Code. This would significantly limit the marketing messages that could be used within the service".

23. There is no proportionality regarding who the code applies to. The code will therefore have the unwanted effect of making it much harder for organisations to provide their services to the UK market or expand their businesses in the UK. The code requires significant resources to be devoted to compliance, especially in creating various age-appropriate versions of the service or by using a "robust" age verification system. This will place unnecessary pressure on businesses of all sizes and in particular those in early growth stages[3]. This would likely create further barriers to growth and establishment of tech businesses in the UK, and thus stifle innovation and employment opportunities[4].

24. If the number of children accessing an online service is an insignificant percentage, there then remains the question of how practical it is for an ISS provider to adapt the service in its entirety to ensure it is age appropriate for that small group. Once more, even if an online service is not directed at children, and has a negligible percentage of underage users, then it simply should not be required to invest significant time and resources into accommodating for an unintended audience. It is not made clear what is considered a significant likelihood of access by children.

25. Furthermore, it is presumed that the code would not only apply to new but also past t in-scope services, no matter how old. In some cases, it may simply be entirely impractical and in some cases impossible to try to make changes to legacy online services to ensure

[2] https://www.asa.org.uk/codes-and-rulings/advertising-codes/non-broadcast-code.html

[3] Over 75% of the 2500+ UK games companies employ 50 people or fewer, https://gamesmap.uk/#/map

[4] The UK games industry directly employs 20,430 FTEs in development, publishing and retail roles, which contribute £1.52bn in direct GVA to the economy. BFI – Screen Business 2019

compliance with the code. This is particularly the case in our sector, where access to e-commerce platforms and games are currently already enjoyed by children and have been for several years with child accounts, parental controls and in line with PEGI age ratings. To now block children from such services unless age verification is complied with, will result in a detriment to such consumers who have previously had access to such services.

26. There is also ambiguity around where the burden of proof may lie when considering platforms versus services (i.e. does the burden lie with the service provider publishing a game/service or the platform on which the game/service is made available?).

27. Finally, we are concerned that the ICO appears to have taken the extreme position that all digital services are somehow inherently harmful for children, and therefore in need of onerous regulation. While presented as a code designed to support compliance with the Act and the GDPR, we believe that the code instead fundamentally shifts the "average consumer" test laid out in the Consumer Protection from Unfair Trading Regulations 2008 to an "assumed child" test requiring service providers to assume that the users of their services are children unless they have robust age-related evidence to prove otherwise. This is not required by the GDPR and to our knowledge is out of step with all other EU countries and other major non-EU markets such as the US and Canada. In doing so, we believe the code enters into the arena of consumer protection and that the ICO may have therefore overstepped its remit.

28. We therefore recommend that the ICO clarifies the scope of the code by giving further detail on what 'likely to be accessed by a child' objectively means, with reference to previous regulatory examples. We also recommend that the design code shifts to a more proportionate risk-based approach where services clearly targeted at children are the priority for regulation. For example, the approach taken by the Office of Fair Trading in their Principles for online and app-based games may better meet the intention of s123 of the Data Protection Act. Under this approach, "likely" is defined as if "*it may be reasonably foreseeable that a game is likely to appeal to children through its content, style and/or presentation*". We also recommend the application of the code in relation to children below the age of consent.

29. We also recommend that the code shifts to a more proportionate risk-based approach where services clearly targeted at children are the priority for regulation. Moreover, evidence of the perceived harms in question needs to be strongly corroborated. There is currently much speculation, for example, about the impact of screen time on children and young people, but little evidence to support a need for additional regulation. We would encourage a more detailed and robust study into the impact of harms and perceived harms on young people as well as concession to the positive impact of online experiences in young people's development

Implementing the code

30. The burden on the service provider to provide "specific, documented evidence" that their services are not likely to be accessed by a child is problematic for all service providers (regardless of size). On top of this, even in the theoretical case that an ISS is able to generate such evidence (which, seems extremely unlikely in today's modern society), it can be immediately lost once evidence to the contrary is found. This would require constant vigilance from an ISS.

31. The code envisages that any ISS used by even a small number of children will effectively have three options:

    (a) apply the code for all users as a default, including adult users (i.e. treat all users as children) even for past content;

    (b) go to the great expense of having separate 'child' and 'adult' versions (with potentially the need to create further versions within the child version to accommodate the code's recommendations for tailoring the offering for differing age groups), with a robust way for all users to confirm their age before accessing the service; or

    (c) implement a robust age gate and bar younger users and/or those users who are unwilling or unable to satisfy the requirements of the chosen method of age verification from accessing the service altogether.

32. For services which are widely advertised but a predominantly adult audience, this may present significant problems. Options (a) and (b) would require expensive additional development for most services, as stated above, may well prevent other new services from coming to market in the first place.

33. Option (c) is not a perfect solution either, especially in light of the code's requirement for data minimisation – since paradoxically, it would require either: (i) the service provider's collection of **more** sensitive personal data from their users than the service provider would otherwise want to, or need to, collect in order to verify their users' ages; or (ii) reliance on for-profit third party age verification service providers who will collect this sensitive personal data.

34. Requiring businesses or their agents to collect more sensitive personal data to comply with the code clearly conflicts with the principle of data minimisation set forth in the code, Act, and GDPR with the potential outcome that many users and parents will be unwilling to provide the information necessary to satisfy relevant verification systems, therefore excluding users from a significant range of services and information that are entirely appropriate for them.

35. The code must seek a balance between its aims of protecting children from real harms, against the need of access to highly beneficial digital services and their positive impact on wider economic and social development. To achieve this, the code should apply to those services that are predominantly targeted towards children. Moreover, evidence of the perceived harms in question needs to be explored. This is acknowledged on page 37 of the code in respect of the addiction debate. There is currently much speculation, for example, about the impact of screen time and social media on children and young people, but little evidence to support the need for government regulation. Indeed recent studies [5]have in fact suggested that the use of social media by adolescents has a trivial impact on their overall life satisfaction and wellbeing.[6] In addition, parents and carers should be allowed to control and direct their children's use of computers and social media. We would encourage more detailed studies into the impact of harms and perceived harms on young people as well as concession to the positive impact of online experiences in young people's development before the introduction of further regulation and guidance.

Age Verification

36. Option (c) also assumes that utilising a "robust" age verification system is simple for an ISS. But this is not the case.

37. The issue is that even for large organisations, a robust age verification system that is also cost-effective and applicable to users around the world does not currently exist, and so all organisations no matter their size will be impacted. Implementing processes to verify passport details or codes provided offline by way of age verification cards, for example, would involve considerable development work for ISSs and the platforms from which they are available. Given the proposed scope of the code, it is a disproportionate proposal that the public will quickly see to be an overbearing and unreasonable distraction of their time and attention simply to use an app. On top of this, if there are increased compliance costs, which may well be passed on to the consumer. We fear it will be UK based innovative and ambitious start-ups who will be worst hit, damaging the UK's reputation as a world leader in these sectors.

38. There are additional issues for an ISS in terms of what appropriate documents would suffice for age verification from global consumers accessing their services in the UK as official documents vary across the globe.

39. Further, the code also doesn't seem to take sufficient account of the fact that there are still a material number of people that would be unable to provide the information required by existing age verification systems (not having passports, driving licenses or credit cards etc.). This carries the risk that implementation of the code as drafted could exclude certain sectors of society from access to digital services. Any negative impact on the availability of, use of

[5] Unicef, Children in a Digital World 2017, RCPCH, The Health Impacts of Screen time, 2019, UK Chief medical Officers' commentary on "Screen-based Activities and Children and young people's mental health" 2019

[6] https://www.pnas.org/content/early/2019/04/30/1902058116

or access to, legitimate digital services would risk significant negative impact on consumer choice as well as the skills, education and awareness of the population with clear consequent risks for the economic and social development of the UK.

40. It is highly questionable as to whether there would be public support for the code, if its likely effect is to cause the unnecessarily widespread implementation of age-verification to control and restrict access to services that, generally, are not viewed as carrying the risk of real harm and that are currently enjoyed by children today with relevant parental/legal guardian consent. It is a disproportionate proposal that the public will quickly see to be an overbearing and unreasonable distraction of their time and attention. Such an impact would also likely damage the UK reputation internationally.

41. We recommend the undertaking of a technical feasibility study on age verification mechanisms to ensure companies would be able to comply with the code. In particular, thought needs to be given to global businesses that are impacted where considerabe development time would be required to design and implement changes required by the code.

Additional comments

42. There is ambiguity around where the burden of proof may lie when considering platforms versus services (i.e. does the burden lie with the service provider publishing a game/service or the platform on which the game/service is made available?). Furthermore, this ignores the parental controls which are widely available for the internet, games consoles, and mobile devices. If strong parental contols are provided by the platform or available from third parties, it should be assumed that parents will use those controls rather than requiring businesses to dramatically redesign their businesses at great cost.

43. Many online services such as consoles, platforms and games have been desigined for global audiences with data privacy obligations in mind for a variety of different regions. Such designs take several years to develop and implement for new generations of consoles and games, with many technical challenges, cost and engineering work. Re-designing such services to take into account the code in such a short timeframe, will be impractical and will materially impact businesses as well as consumers who currently use such services.

44. We recommend that how the code defines when a service is “likely to be accessed by a child” is reconsidered. For example, the approach taken by the Office of Fair Trading in their Principles for online and app-based games may better meet the intention of s123 of the Data Protection Act. Under this approach, “likely” is defined as if “it may be reasonably foreseeable that a game is likely to appeal to children through its content, style and/or presentation”.

The Code:

We now address our comments on certain of the code's 16 specific standards of age-appropriate design.

Best interests of the child: *"The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child".*

45. Whilst putting the best interests of the child at the heart of any ISS design is a worthy ambition, we are greatly concerned about the practical implementation and implications of such a broad scope. Treating all services that could ever be accessed by a child as in scope is an unjustifiably broad interpretation of that concept and will lead to an unworkable code and possible litigation.

46. Our sector are hugely supportive of ensuring that there is fair processing of children's personal data in compliance with the principles of the GDPR, including taking into account the standards that are issued to protect the processing of children's personal data, where appropriate to their services.

47. However, the Code seeks to impose the standards and principles of the United Nations Convention on the Rights of the Child ("**UNCRC**") on all ISS providers despite many of them not being subject directly to UNCRC and particularly where not all principles of UNCRC relate to privacy.

48. Some ISS simply are not designed for children and this is a completely valid creative choice. The code guidelines essentially state the code must be fully abided by if there is even the slightest risk of a child accessing an ISS. That means that all ISS must be designed with children as a primary consideration – even if that simply is not the creative choice they wish to make.

Age-appropriate application: *"Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children."*

49. The proposed age ranges put forward could potentially further confuse matters by adding additional complication to design process, marketing and user experience. ISS providers may have difficulties in ensuring their T&Cs are accurate whilst understandable for a child in the 0-5 age group.

50. This could make the consumer experience more complex not less, and there would be difficulties in deciding on which iteration of the service would front marketing. It also risks introducing vagueness to an area which in principle ought to be simplifying issues. Further, with child development occurring at different rates with different people, and with cultural and social differences playing a part in child development, apportioning age ranges risks introducing further uncertainty.

Member quote: "We would have to write our T&Cs and privacy policy in language which could be understood by a range of different age groups (from 5+ upwards) simultaneously, which will be prohibitively costly. There are often complex inclusions in T&Cs which are required by law, and it is not always clear if these can be simplified for a child audience while fulfilling the legal obligation."

51. As with other areas of the code, the burden on all businesses, regardless of size, to potentially design their ISS with five age ranges in mind would require significant investment, which in turn could stifle innovation and deter businesses from starting up or expanding. Robust parental controls are already provided by platforms or are available for parents to install on devices used by children. For example, many services that are offered globally are designed to allow parents to set up accounts for children under 18. This puts the contol in the hands of an adult.

    It should be noted that there may be some services which allow the child to consent (which have taken into account the various derogations that GDPR permits EU member states to make in relation to the age that children can provide valid consent that could vary from ages 13 to 16). By implementing the provisions of the coode, this may inadvertently restrict access to such services where children under the age 18 are legally able to provide their own consent but would still have to treated as a child.

52. We would like clarification on what is meant by a 'robust age-verification system'.

53. In addition, there is an implicit assumption that data collection and processing is harmful without sufficient weight afforded to the evidence base. In the games industry in particular, non personal or anonymised data collection is fundamental to the delivery of improved content including fixing bugs or problems that users have highlighted to ensure their game play is more enjoyable. More thought needs to be given to the purpose of data collection in these examples.

Member comment

"It seems to me that with any 18 rated game, the ICO's "alternative" to the age-verification or impractical privacy restrictions (treating all players of a mature game as children), would require the publisher to design different versions of a game, geared towards age groups which are below the age-rating for the content. Further, the Code requires the publisher to design its communication with the user (privacy policies, terms etc) in a form appropriate for the relevant age group (including using diagrams and videos etc).

This means that compliance with this "alternative" would require the publisher to make versions of an 18+ rated game that are designed and presented as more user-friendly and accessible for children and intended, specifically, to be provided to relevant children who have self-verified their age. This would be both irresponsible as a content provider and likely to cause conflict with other regulatory requirements.

This means that the only practical courses of action available to publishers of 18+ games (or in fact any games subject to age ratings) is either to accept the burden of applying the full extent of the Code to all users (with the inherent negative impacts, including on the quality of experience for the user and the commercial rights of the publisher) OR to implement "robust" verification systems, as yet unavailable, with all the potential risks and barriers to access as discussed.

As far as I am aware, there is no industry or governmental regulation of games content worldwide that requires the standard of age-verification proposed here…. The vast majority of games are rated to provide specific information for users and parents. Those ratings have consequences for the marketing of rated games. Where the publisher is in compliance with all codes and laws designed to regulate the marketing and distribution of rated games, it should be fair (especially using a risk-related approach) for the publisher to apply the already comprehensive provisions of the GDPR on the basis that the Users are of the age for which the content is specifically directed."

Transparency: *"The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated."*

54. The requirement to provide clear, intelligible, comprehensive and transparent information on such issues as the type of information collected, the purpose of the collection, and the terms and conditions of service is to be encouraged. However, a balance must be struck between the provision of bite-sized explanations and age tailored information with the

requirments of GDPR as just one example.

55. As with many other areas of the code, it might not always be practical for companies to provide numerous versions of such information for different age-groups and there is clear potential for this to create more confusion if there is a lack of consistency. Similarly, the suggestion that ISS include videos or audio explanations of privacy (and other consumer facing) terms, would be unworkable for apps distributed via the App Store or Google Play Store given the requirement for apps to include all such terms within the app itself. Building in such audio-visual features would result in the size of the app's download file increasing significantly, which would make downloading it onto most consumers' mobile phones or tablets extremely problematic. It will also cause many platforms to become more cumbersome where it has to providedifferent explanations against each control for each age range not to mention the development, time and cost to build such features into existing platforms, consoles and games.

56. The code does not discuss the role of education and skills in helping to explain concepts increasingly relevant to the Fourth Industrial revolution. There needs to be greater emphasis in providing children and young people, parents and teachers with the educational resources necessary to fully understand these concepts as well as their implications before placing burden on ISS to tailor the information they provide.

Detrimental use of data: "*Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice*".

57. Our members that provide ISS are already working within and are compliant with existing statutory regimes, from the requirements of the GDPR, the CAP Code for marketing, Age Ratings (The Pan-European Games Information "PEGI" is legally enforced at retail in the UK) or relevant elements of European Directives such as Audio Visual Media Services Directive. In addition, and particularly in the games and interactive entertainment sector, self-regulation through parental controls (linked directly to the PEGI age-ratings), in-built safety features and tools etc means that, with the proposal to implement default "high privacy" data settings for all users, there is a potential for the code to undermine existing activity and increase costs associated with it.

58. We are also concerned that the examples given under this principle, of requiring platforms and games to add pause buttons and warning against any feature which encourages players to keep playing, goes beyond the ICO's remit of data protection and strays into content regulation. Games developers naturally focus on making their games as fun and engaging as possible, which this principle seems to suggest may be against data protection law. More appropriate measures would be to provide more education on such perceived detriments to parents/legal guardians, who are more able to ensure their children take the required

breaks.

59. We recommend that the code fully reflects the UK's obligations under the UN Convention on the Rights of the Child (UNCRC) relating to privacy[7], but balancing the right to privacy against the other rights of the UNCRC.

Policies and community standards: *"Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies*)".

60. The games industry has a well established practise of community management with extremely high standards. The industry has good examples of how these communities are central to protecting players from online harms. Further information on this can be found for example in our response to the Government's Online Harms Green Paper and will be included in our response to the Government's Online Harms White Paper[8]. Care must be taken with the code that it is consistent with the direction and intention of the Online Harms White Paper. Furthermore, providers should not be penalised for failing to uphold other terms, policies, rules or standards that are not a specific requirement of the GDPR and in particularly Article 5(1) of the GDPR. We would also refer you to our comments under "Age Ratings" at the beginning of this response.

Default settings*: "Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child)."*

61. In our response to this particular point, we will only focus on the use of parental control settings and whether these should be off or on by default. You can see our response on general user settings below.

62. In addition to clear age rating symbols and descriptor icons, all of today's consoles, PCs, handheld games devices, and mobile devices offer parental controls. For example, many consoles require someone over 18 to open a full access account, with parents and guardians then able to create sub-accounts for their children with built-in safety features including communication restrictions, web filters, locks on non-age appropriate games, time limits, restrictions on sharing games content on social media and parental and guardian monitoring tools. Using parental controls not only offers parents and carers a greater degree of control but provides families an opportunity to agree how they will play games. This can then be implemented on each system automatically without creating all the secondary problems for businesses noted above.

63. Parental controls are much easier to implement. Introducing individual privacy settings for users on multi-user devices can be problematic, particularly for PC users. It would be difficult

[7] https://www.unicef.org.uk/what-we-do/un-convention-child-rights/

[8] http://ukie.org.uk/sites/default/files/cms/docs/Ukie%20Internet%20Safety%20Strategy%20Response%20pdf_0.pdf

on a PC to implement multiple privacy settings especially for accessing and storing cookies given a provider of ISS's distance from the development of the PC and web browser.

64. Further, Ukie and its members support the use of active choice by parents and carers, as opposed to default on for the entire population, for internet-enabled devices. As Dr Tanya Byron argued in her 2008 report, it is more effective to ask parents 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[9].

65. We agree with the Byron report's conclusions on active choice, and it is the route we believe should be taken by ISPs (as we recognise is happening) and by internet-enabled devices such as games consoles: the user should be told what the available controls are and given the choice to use them – a choice they are actively required to make in order to use the device for the first time, either by means of warnings/notices or by options presented during device set-up or registration process.

66. We support this approach for two reasons in particular: (1) the principle of active choice already has a consensus of support amongst console-makers, and (2) any changes they are required to make should be given a long lead-in, due to the large timelines now between the release of each new generation of games consoles.

67. We would, however, discourage reliance on one sole solution to this problem; active choice should not be mandated as the only solution available. The games industry believes that there is no single answer to protecting children. A combination of solutions, including at a device level, at a services level and at an ISP level will offer the maximum protection. However, the constantly evolving nature of technology and internet-based services mean that any solution will not be permanent. Educational campaigns sponsored by industry will become even more important to continuously inform children, parents and our players on how to enjoy a fun, safe, fair and inclusive games' experience for them and their families

Geolocation: *"Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session".*

68. Geolocation data is an important tool for providing innovative new products and services and has key implications for providing security features. The games industry has pioneered this emerging technology to great effect without compromising the safety of its players.

[9] Dr Tanya Byron, "Safer Children in a Digital World", (2008).

69. It is also an important tool for providers to understand the interaction with their services at live events (such as conferences, exhibitions) as well as to improve a user's experiences for future events. Most of these events would be attended by children with their parent/guardian and on these occasions if there is transparency to users, geolocation tracking would not be a detriment to the safety of children.

70. User consent is already required as part of PECR, and services must make it clear what their location data will be used for when they prompt for a user's consent. We hope that 'switch geolocation options off by default', does not mean that a user is not easily given the opportunity to consent to geolocation services as soon as they log into a platform – geolocation services which may enhance their experience of an ISS. Some online services rely on geolocation to even operate – the code's broad scope means that, at risk of sounding repetitive, services not even aimed at children will have to have geolocation options off by default, including when geolocation is used for security reasons (e.g. to notify a user there was a log in from an unfamiliar location).

71. The assumption that all users are children by default and expectation that children would have to actively find and change the default setting to enable geolocation tracking may have unintended effects. For example, it may encourage a child to be granted access to other default settings on devices designed to safeguard them such as spending limits, time limits and specific types of content filter.

Parental controls: "*If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored*".

72. The games sector has worked hard to provide robust and effective parental controls to help ensure a safe and healthy playing experience. We agree that providing children and young people with appropriate information about how these tools may track and monitor their online activity is an important part of respecting a child's right to privacy. We believe that informing parents, carers and players of the availability and functionality of parental controls is fundamental to the effectiveness of the controls themselves. Parents should be given the freedom to utilise parental controls how they see fit, rather than requiring businesses to dramatically redesign their businesses at great cost. A balance must however be struck in terms of providing information and equipping people with the knowledge to bypass the controls.

Profiling: "*Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)*".

73. What is meant by ‘profiling’ is not clear and we ask for a less ambigious sense of what is meant by it in order to ensure that other iterations of profiling are not included. In games, “profiling” does not necessarily mean profiling data processed by a third party for advertising analystics – it is usually analysing data and tailoring content in order to improve the game experience. This might include, for example, fixing areas of a game that prove problematic to progression or targetting content according to appropriate skill or experience level. It may also include gathering information on what features users enjoy the most so similar additional content can be created.

74. Additionally, it can benefit users by allowing providers to not display content to a user that they may have already purchased to avoid them purchasing that content repeatedly. Some profiling may improve a user’s overall experience – for example, recenly played games can be remembered and displayed to the user at log in. These benefits will be lost if options are set to default.

75. Introducing specific notices on how profiling is used as well as separate privacy settings for each different type of profiling for all different age ranges, will require increased development work for providers of ISS as well as increased cost, that will be impractical to implement within the timescales. This may in turn cause services to be cumbersome to navigate, which may be a detriment to a user’s experience of a service that they have used without such notices to date.

76. Profiling settings should be placed behind parental controls as it is for the parent/legal guardian to decide what is appropriate for their child, along with transparency notices in a child appropriate language to explain the consequences of such a setting to a child. The child should be provided with an option to switch off a profiling setting that has been turned on by a parent/legal guardian if they wish to do so.

77. Prohibiting service providers from profiling their users unless there is a “compelling reason” for such profiling and is a very high bar to clear, particularly given the examples set out in the code (i.e. child protection and safeguarding). Further, the suggestion that separate options should be given for each use of profiling also ignores the numerous alternative legal bases that service providers may rely upon under the GDPR in favour of a purely consent based approach which may well lead to consent fatigue.

78. Article 22 and recitals 38 and 71 of the GDPR contend that the automated processing of data involving children and young people is not prohibited as long as it safeguards the subject’s rights and freedoms and legitimate interests and is necessary for the performance of a contract. Profiling might, for instance, help improve the game experience by fixing areas of a game that prove problematic to progression.

Nudge techniques*: “Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use. “*

79. As with other areas of the code, the broad definition and set of assumptions associated with the use of so-called nudge techniques potentially misses some of the reasons data collection might be used. As a result, this may lead these legitimate practices being sidelined so user experience suffers

80. The ICO seems to imply that online services only seek to encourage users to stay actively engaged with a service to maximise the amount of personal data that can be collected. Rewarding users for progressing within a game is part of the industry's DNA and a basic condition to ensure that the game experience remains competitive and enjoyable. Care must therefore be taken in enforcing this Code that the positive and legitimate practices used by the games industry are not effectively outlawed.

Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

81. Our sector is completely supportive in enabling users including children to exercise their data protection rights and reporting concerns as part of the GDPR compliance requirements. Providers already explain to users how they can easily access their personal data as well as exercise their rights.

82. Implementing online tools for children to download all their personal data or exercise their rights will require many providers of ISS who currently do offer such online tools, to carry out more developmental work and incur cost in building such tools to enable such functions. There could be unforeseen implications of such mechanisms, whereby a child accidentally presses an icon to exercise their rights or to download their data, when that is not actually what they wanted to do but as a consequence it places a further administrative burden on businesses to fulfil alongside requests from consumers who genuinely want to exercise their rights.

Data Protection Impact Assessments (DPIA): Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

83. A DPIA is clearly an important requirement to ensure that products and services are appropriately assessed for high risk processing of personal data. In many cases, it will be appropriate and necessary to seek and document views of children and parents and take them into account for the design of a service or product. However, in other cases, it may not be appropriate particularly where there may be commercially sensitive development designs at early stages, meaning that businesses would not be able seek views without giving away commercial secrets of a design which could significantly compromise their future service. Imposing research measures in all cases are also likely to also increase the administrative burden on providers along with compliance with statutory legislation and codes of practice.

Conclusion

84. The purpose and aims of the code are admirable to ensure the processing of child's personal data is completed lawfully, transparently and fairly. However, the code does push the boundaries of the GDPR in relation to the processing of personal data in some areas, creates many challenges and undesirable consequences as identified above. Further consideration and thought needs to be taken into account for each industry affected by this code to ensure a fair and appropriate balance is drawn.

85. Additionally, more focus should be placed on:
    - education and parental oversight in teaching children to understand how online services work;
    - how parents and children can manage their online lives safely and securely; and
    - ensuring providers of ISS take responsibility to empower parents and children in these areas in relation to their products and services.

86. We finally strongly recommend the maximum implementation period available when the code comes into force, to ensure companies have time to adapt to the new requirements.

87. The Code will have significant economic implications for UK businesses offering services 'likely' to be accessed by a child. Given the number of platforms and offerings affected, the financial and technological implications of remediation efforts, the risk of significant sanctions, the short implementation period and the competitive disadvantage for some UK based companies (when compared to competitors offering similar services from outside the UK), the Code may result in a reduction of offerings to UK children and/or companies choosing to publish their global offerings from locations outside of the UK - to avoid the collection of children's data from multiple jurisdictions becoming subject to the Code.