Information Commissioner's Office

Consultation:

Age Appropriate Design code

Start date:15 April 2019

End date: 31 May 2019

ico.
Information Commissioner's Office

Introduction

The Information Commissioner is seeking feedback on her draft code of practice Age appropriate design - a code of practice for online services likely to be accessed by children (the code).

The code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet.

The code is now out for public consultation and will remain open until 31 May 2019. The Information Commissioner welcomes feedback on the specific questions set out below.

Please send us your comments by 31 May 2019.

Download this document and email to:
ageappropriatedesign@ico.org.uk

Print off this document and post to:
Age Appropriate Design code consultation
Policy Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation please telephone 0303 123 1113 and ask to speak to the Policy Engagement Department about the Age Appropriate Design code or email ageappropriatedesign@ico.org.uk

Privacy statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public or a parent). All responses from organisations and individuals responding in a professional capacity (e.g. academics, child development experts, sole traders, child minders, education professionals) will be published. We will remove email addresses and telephone numbers from these responses but apart from this, we will publish them in full.

For more information about what we do with personal data, please see our privacy notice.

Section 1: Your views

Q1. Is the '**About this code'** section of the code clearly communicated?

No

On the whole we would agree that this section is clear. However, we would like to make a few observations.

The code makes clear that this work has come from the General Data Protection Regulations that sets age restrictions to the age of 18 with consent in the UK set at the age of 13. The 16 standards of design are also very clear and it has been made clear that these will be the reference to which the ICO will look when making judgements about whether an ISS has appropriately safeguarded a child's data.

However, the code is restrictive in some of the level of detail whilst being vague in language in a number of places. This will cause difficulty in understanding, and therefore implementing, the code for businesses. There is no definitive framework of rules provided by the code which companies can follow to satisfy a regulator in case of future investigation. We would prefer very precise guidance if it continues to be on a granular level with clear examples of what will and will not be acceptable by the ICO.

Alternatively, we would support the 16 code principles against which you will judge whether a company is acting responsibly. These overarching principles are set out in the GDPR and companies will have already invested in complying with those principles in the lead in to the deadline in 2018 and beyond. We would support the code simply stating these 16 principles and then allowing companies to assess their behavior against these and finding their own routes to compliance which are clearly laid out in a DPIA. The code as it stands falls between these two concepts. We would ask that companies are given more flexibility to determine the way in which they comply with the GDPR.

Giving companies 61 days to verify all of their ISS comply and to make relevant changes will be unfeasible espescially with regards to age of digital consent which would entail companies conducting large scale audits of their ISS. The complexity of what is being asked and the time it will take to assess every ISS and determine if it is in scope, what changes are needed and time to implement those changes will take longer than the 61 days suggested as the time frame in the code. This time frame might work for a company with one ISS but for companies who have children and parents as their main customers this will be a significant body of work. Toy companies may have services for parents, for example a website with toys and play discussion for children under the age of 5. This site is not targeted at children but their parents. Just because it contains images of toys the toy company will need to make a judgement about 'appealing' to a child – therefore likely to be accessed, they will have to undertake an assessment, a DPIA, decide to make changes and implement any changes – they will have to do that across every service they offer with every age group of user. We would ask for a significantly longer transition period for any changes to legislation in this area. For "hardware" changes we would also require additional transition time (please see our specific section on connected toys). We would ask that the transition period to bring in new regulations is set at the maximum statutory time scale of 12 months.

Currently the code suggests all websites will have to age gate their content. It appears that every website, even if content has clearly been written for adults, will have to age gate visitors to be able to prove they are over the age of 18 or will have to apply

these rules regardless of the fact children are not the audience. It was taken, when meeting you, to understand that this is not the intention of the ICO and we welcome more clarity in the final text on how companies can make those judgements.

This would add a great level of burden to companies and would result in adding cost and complexity without adding greater levels of security for children who were not the intended audience in the first place.

In our meeting you explained this was not the intention, that you do not expect to AV all users and that a DPIA should be done to assess whether AV is required in "high risk" scenarios. If determined not to be high risk the alternative would be to make privacy setting the highest from the start with age appropriate (judged on a user self selecting) privacy wording allowing the user to deselect the highest settings as long as the company is transparent in how the data will be used and in return for what functionality and that this has been determined to be acceptable justification in a risk assessment done by the company under their own DPIA. We welcome this clarification and would ask that this is made clearer in the code. We would ask that the code clarify that AV will not be needed in many scenarios.

We would ask that the code give examples of high risk scenarios – guidance on what companies should be assessing to determine risk.

Ability to advertise – we welcomed your clarification in our meeting that you have no intention of banning marketing to children or their families, that this is not in scope and was not an intended consequence of the ICO code. We would welcome this being made clearer in the code.

We understand from our discussion that age appropriate marketing can continue and that there is no intended ban on profiling. We discussed the self declaration ages given on contact with an ISS can be unverified, that these ages could be used to deliver age appropriate marketing / advertising and that profiling is allowable to be able to deliver age appropriate advertising so long as this is done within the GDPR principles of being honest

and transparent and a company can evidence their risk assessment of the activity. We would ask that this is made clearer in the code.

Age of user – as part of our discussions on age verification we discussed the concern of the industry that all toy ISS would be within scope and open to the ICO determining they could all be 'accessed by a child'. We would ask for more clarity in the way the ICO will make a determination on this. We explained the burden this places on toy companies to have to cater for all ages on all services. We discussed companies being able to assess content and determine from a risk assessment, the age to which they should target language and communcations, type of toy or service (ie a toy suitable for being played with by a 9 year old not having to cater to an under 5 in the language, supporting website, privacy information as the whole experience would not be aimed at that age). We would ask for this to be made clearer in the code. We also discussed some of the ways the ICO would determine the age-appropriate for the content on a child site and that language, advertising etc would all be looked at to be able to determine the target age for a site overall. We would welcome clarity in the final text on this.

When outlining the consequences of non-compliance of the code, we believe the range of sanctions and particularly fines, are not in line with the offences and would likely cause serious damage to a UK business. Since 80% of toy companies are SMEs or family owned, the likely average turnover of a manufacturer is towards the lower end of the research found in your consultation document. A fine of €20 million (or the threat of one) would remove competition from the market and should a fine be enforced, wipe out most businesses in the market. We would propose removing the €20 million maximum fine and restricting the fines to 4% of UK turnover.

Q2. Is the '**Services covered by this code'** section of the code clearly communicated?

No

We welcomed, in our meeting with you, your willingness to make clarifications in this section regarding the scope, the legal definitions of an ISS and the legal definition of "likely to be accessed". We would

welcome these clarifications as we believe greater guidance is needed on what the threshold is for when an ISS will be considered 'likely' to be accessed by children and what percentage of audience share etc would be considered significant.

We would ask that perhaps some of the exemptions are made clearer at the start - i.e. making clear in this section that closed-loop systems, ones that only store data on a local device, websites that may appeal to children but do not track or capture data, are not captured by the regulations. Perhaps adding a section that explains "if you do / do not do the following you are not captured by the regulations". We believe many SME's who do not have the resource to undertake this complex and expensive code would prefer to build in rules at the beginning that exempt them, i.e. they may make changes that mean they collect no child data in order to not have to comply with the code. Of course, this gives a greater competitive advantage to large companies with more resource, however we believe that many SME's will make that choice, as we know many in the toy industry have done already. Making it clear in the code what behaviour exempts a company would be helpful for these SMEs.

We would also like the "connected" device made clearer in definitions, i.e., if a device ONLY stores data locally currently this is out of scope - we agree with that definition. However, clarity around data subsequently being uploaded by the user such as social media accounts should be clarified as a separate action and not part of the device experience or influence.

Standards of age-appropriate design

Please provide your views on the sections of the code covering each of the 16 draft standards

1. 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.

2. 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.

3. 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.

4. 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.

5. 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).

6. 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).

7. Data minimisation: Collect and retain only the minimum amount of personal data necessary to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

8. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

9. 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.

10. 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.

11. Profiling: Switch options based on 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).

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

13. Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable compliance with this code

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

15. Data protection impact assessments: 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.

16. Governance and accountability: Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code

Q3. Have we communicated our expectations for this standard clearly?

1. **Best interests of the child**
No

This is clear however the BTHA believes the best interest of the child is being given the right to information, opportunity and choice as well as privacy. The restrictions in this code will not lead to the best interests of a child being served as their choice of free content will be severely limited by the way the code is currently worded. We welcome the reworking of the code to lift the restrictions which would effectively ban marketing and the legitimate collection of data that adds to enhanced gameplay and child experience.

2. Age-appropriate application

No

We generally support the requirement to provide information to users about the processing of their data in clear language. However, the specific requirement to deploy bite-sized just-in-time notices, specifically tailored to approximately six different age-ranges (starting from 0-5 years old), each time the "use of personal data is activated" presents significant operational challenges. For instance, it is difficult to imagine how to make a user under the age of 5 understand the difference between essential and non-essential processing, regardless of how it is presented (pgs. 29-30); or whether a change in their privacy settings should be permanent or returned to the high privacy default (pg. 44).

We do have concerns about the age of 18 now being the parameters by which we are governed having already worked towards the UK guidelines of the GDPR age of 13. The code requires companies to target age ranges of children likely to access services and apply the criteria of this code to them once age verification has been done, however, it does not go far enough to explain how the age range of children likely to access these services should be accomplished. The BTHA requests clear examples of mechanisms which will be considered acceptable methods for verifying the age of children and then assessing which age of child an ISS can be targeted at. Until the ICO can signpost an independent and affordable age verification tool then the legislation will be flawed and impossible to comply with. Even when there are such systems we would ask that these are free of charge to users otherwise they will be a barrier to SME access. Organisations will, as a resulf of the code, need to collect large amounts of additional data, often highly sensitive, such as official identity documents solely for the purpose of meeting ICO guidance. In our meeting you did explain this was not the intention and that simply self selection of a range of age by the user would suffice - we would welcome this clarification in the final text.

We believe we need greater clarity on how we can make age appropriate content if we constantly need to default to the youngest setting. "Taylor the measures in this code to the age range of your users." How can this be done if we are unable to request the age of the child and the

preferences are turned off by default? We welcome the ICO determining that more information will need to be added to the code to clarify these concerns. Also, it will be difficult to settle on what users in each band will need in terms of privacy and we would welcome more guidance on this from the ICO.

There is no proportionality when considering intended audience, the type of services offered or how high the percentage is that the likely audience is children, as well as regarding the size of the company offering the service.

The code needs to be far clearer in how it expects an ISS and a connected toy to cope with using multiple age bands across product and service design. Clear guidance will be needed by the ICO on what will be needed by users in each age band in terms of privacy (as this is already problematic in terms of plus and under 13) but also how that translates in regard to business products and services. The BTHA welcomed the guidance in our meeting that companies would we be able to target a service to one age bracket to avoid having two or more tiers of protections as long as that was clearly laid out as part of thinking in a risk assessment as part of the DPIA. Clarity within the final code would be most welcome to ensure companies understand this is permitable.

3. Transparency

No

The BTHA understands that the GDPR requires that all children are provided with information in a way in which they can access and understand it, however, to achieve any understanding of data approval in a child of 6 months, for example, is unworkable. For the youngest age group we would ask that parental privacy statements are the accepable provision (for under 5s).

Indeed, in trying to determine the possibility of toy companies undertaking the provisions in this code we sought expert opinion on this requirement. Dr Amanda Gummer, a child development expert stated, "Children under the age of 8 are unlikely to have the social or cognitive ability to give informed consent due to their lack of understanding of concepts such as permanence, the reach of the digital world, or the motivations of corporations. Parental consent would be an appropriate vehicle to use for young children’s data and online engagement, but I believe there is little any company can do to obtained informed consent from children under 8 directly".

We would ask that the ICO accept parental approval of privacy settings, certainly for the under 5s, but would ask for consideration above this level to the age of 8 years.

We would ask for additional clarity on whether the ICO's example of good practice on page 30 means that the given wording be used exactly?

Upscaling/Downscaling – to what extent should companies provide upscaled information on the details of their data processing practices? If a site is intended for older children and adults, how far should user be able to downscale? For example, to what extent are companies expected to scale to, particularly if a toy or service is clearly for a particular age range? We would concerned about having to do this with a physical toy. We welcomed your thoughts in the meeting that if a toy can reasonably be shown, and documented in a DPIA, to be for a particular band of age group that you would consider that to be the target age for the information and language provided. We would welcome clarification of this in the final text.

We believe the suggestion to use icons and symbols could lead to the creation of multiple different systems. We believe this could lead to confusion amongst parents and children when moving between ISS and would welcome ICO central messaging for companies to refer to.

4. Detrimental use of data

No

We would ask for more clarity or a central area on the ICO site that is kept up-to-date with recommended areas of child data collection that have been shown to be detrimental to their wellbeing - this open ended and precautionaryapproach gives no safety net or assurance to companies that are investing in doing the right thing only to find the parameters change. This area needs to be clarified and perhaps adopting a code of practice on marketing and advertising or profiling for example would be much more concrete and useful to data controllers. Certainly concrete data and examples are needed from the ICO.

5. Policies and community standards

YES/NO.

If NO, then please provide your reasons for this view.

6. Default settings

No

"High Privacy" needs to be more clearly defined. Clarity should be given on whether there are circumstances under which default settings do not need to be set to the highest setting.

It would be helpful to gain clarity on what happens if defaults are reset to high privacy for existing users. For example if users have already set their privacy limits will these need to be changed back to high privacy when the code comes into practice or will their previous (prior to the code coming in) settings be acceptable? Will the code only relate to new users to a service? Will a question to existing users such as "would you like to review your settings" suffice?

7. Data minimisation

No

The code needs clarification to explain that it is possible to collect data, for example to deliver a free service with advertising, as long as that is done under the guiding principles - which would involve being transparent and honest about the data being collected and verified in order to provide the free age appropraite content or service to customers.

Companies need to have a 'ball-park' figure for a child's age to be able to target age appropriate warnings and should be allowed (as long as the correct permisions and privacy notifications have been given) to use this data to deliver safe and age appropriate advertising and content. We welcomed the ICO clarification of this point when we met, but would welcome clarification in the final text.

8. Data sharing

No

We would ask that the final code reflect the ability for companies, as long as they are honest and transparent in collecting data and gaining the correct level of consent and explaining what it will be used for - to be able to deliver age appropriate content and advertising. The Code requirement of a "compelling reason" (page 52) needs to be defined more clearly and outline whether it will allow for the use of data to be used to personalise experience on the app or website.

9. Geolocation

Yes

We would ask for more detail about permissible uses, for example, would a toy that uses geolocation technology for a multiuser digital tag game be considered to have a compelling reason for using geolocation?

10. Parental controls

Yes

11. Profiling

No

Under this draft of the code, companies who do not presently profile for age criteria are now expected to do so, i.e. requesting more data than normally needed, or risk non-compliance. Please could the final code reflect the ICO's position on what is and is not allowable and how this fits with the data minimisation principles.

12. Nudge techniques

No

If companies outline what they believe as the value of sharing additional data, for example if the service being offered is a positive, valuable one, we believe this should be considered permissible.

We would like to be able to communicate in a positive way about what we see as the value of sharing additional data without this being considered a nudge.

We would ask for a clear line distinguishing "sticky" fun game features that are not prompting users to give up personal data and game tuning that might be reactive to a player's play style and provide more or less of certain options in a game. Is offering rewards to complete things faster a nudge? Is tuning game play based on purchase or play patterns a nudge? We believe this type of activity should be excluded if this does not ask for a player to divulge additional data?

13. Connected toys and devices

No

Connected devices need to be subject to different /additional timescales and rules. As a note here the BTHA has had a connected toys guide for members since October 2017 to help them when developing connected devices which covers data protection as well as cybersecurity, mechanical properties etc.

We believe there to be a number of areas of the code which need to be changed in regard to devices.

Firstly, we appreciate the explicit exclusion of a device which only stores data in the device and does not connect to the internet. We would like clarity in a related area however.

If a child were to store videos on a device, the device itself does not connect to the internet, but the child then takes the content and uploads that themselves - would that be excluded from the scope of the code? We would ask that it is excleded and made clear in the final text.

The code is asking for an icon at point of purchase. This is a reasonable request but will take time to achieve on a physical product - on Page 79 the code lays out the requirements for an icon or information on packaging. This will not be possible in 61 days. Toys take 18 months to 2 years to develop from beginning to market shelf. Clearly new requirements on software should be able to be uploaded as an update, however there should be awareness of timescales for "hardware' development. Companies will have developed products to the GDPR requirements but will not have seen these current code requirements before. Toys need factory time plus three months shipping at sea meaning that a minimum of 12 months would be needed for toy companies to ensure they have an icon on packaging and hardware requirements (such as the light up when connected) built in.

Changes to design and packaging will also cost companies money as even after the minimum timeframes they will need to rework packaging artwork or toy design. This can of course be done but the longer companies are given to incorporate this into initial designs the less burdensome the changes become.

Many toys are made out of season to be able to meet demand at Christmas. Therefore this Christmas' connected toys are being manufacturered in China in the next month for storage before being shipped to retail from October.

We would ask that changes in this legislation follow other toy safety timelines, for example toy safety standards have a transition period that begin from the moment they are written in as statutes. This allows companies time to understand and comply with the new requirements and to make the necessary changes without incurring more cost than is necessary and allowing them to communicate any changes that are necessary to both suppliers and their customers. That period is usually 6 months to one year. We would ask for a year in this case due to the redesign, remodelling and tooling that would be needed in this case for the physical product design.

A separate issue is sell through of product. Once the new code is published there will be product on the shelves in the UK that is made to comply with the GDPR but again will not have been made to this new requirement. There should be an acceptable sell through period such as the rules relating to "placed on the market" items under the EU Blue Book definition. This definition will be recognised by both companies and enforcement as it is a tried and tested method that has been used when there are new safety standards.

We notice in the supporting information that the statement is made that connected toys are most used by the under 5 age group. This is not the

experience of the toy industry. There may be devices for this age but the majority are for older children. An accompanying document has been attached to this to demonstrate the likely age of a connected toy based on the top selling toys of 2019 so far.

14. Online tools

No

The guidance in this section suggests that for a 0-5-year-old companies should "provide icons that even the youngest will understand'. We would contest that this is possible to achieve in an area as complex as data protection. We would ask that the code recognises that getting a 3 year old to understand what data is, what it does and why it is collected is possible and that, given we need parental consent at this age anyway, that for pre-literate children parental guidelines are sufficient (see transparency above for more information).

Should the ICO deem this not to be enough and 0-5 guidelines are required we would ask that the ICO have a central site with examples of what would be deemed acceptable and understandable for a 0-5.

15. Data protection impact assessments

No

Certain aspects of the proposed Code go far beyond data protection requirements. For example, Standard 15 on Data Protection Impact Assessments (DPIA), requires companies to consider "broader risks to the rights and freedoms of children, including the potential for any significant material, physical, psychological or social harm" (page 83), as well as issues like self-esteem, peer pressure, encouraging excessive risk-taking or unhealthy behavior, excessive screen time, and interrupted/inadequate sleep patterns. (see page 87). Including these considerations would fundamentally change the nature of DPIAs and would broaden their application well beyond the data protection purposes of the GDPR.

The requirement to consult with parents and children as part of a DPIA is a huge burden particularly for SMEs and could be very costly given toy companies are likely to be found to be likely to be accessed by a child simply by virtue of being a toy company (although above we ask for clarification on this issue as we can see this will place massive pressure on the toy industry overall) - even if communications are far more likely with parents in many cases. Therefore toy companies are likely to have to do a DPIA for every website, app, toy or service they develop and as part of that will have to undertake research or consultations. This is a very onerous requirement and we would ask that it is reworded to suggest consultation should be considered as part of the overall DPIA but that companies will not be held accountable on the absence of such research. This requirement is very cumbersome and costly and will lead to UK

companies being less able to compete on a level playing field with other EU and worldwide companies.
16. Governance and accountability
Yes If NO, then please provide your reasons for this view.

Q4. Do you have any examples that you think could be used to illustrate the approach we are advocating for this standard?

1. **Best interests of the child**
No If YES, then please provide details.
2. Age-appropriate application
No If YES, then please provide details.
3. Transparency
No If YES, then please provide details.
4. Detrimental use of data
No If YES, then please provide details.
5. Policies and community standards
No If YES, then please provide details.
6. Default settings:
No If YES, then please provide details.
7. Data minimisation
No If YES, then please provide details.
8. Data sharing

No If YES, then please provide details.
9. Geolocation
No If YES, then please provide details.
10. Parental controls
No If YES, then please provide details.
11. Profiling
No If YES, then please provide details.
12. Nudge techniques
No If YES, then please provide details.
13. Connected toys and devices
No If YES, then please provide details.
14. Online tools
No If YES, then please provide details.
15. Data protection impact assessments
No If YES, then please provide details.
16. Governance and accountability
No If YES, then please provide details.

Q5. Do you think this standard gives rise to any unwarranted or unintended consequences?

1. **Best interests of the child**
Yes

As a general overarching principle, a child's right to privacy should be balanced with a child's right to information, opportunity and a choice of content. Much of that content will be driven by free advertising. We would ask that you consider the detrimental impact on breadth of choice under the current code. The code has in fact placed such restrictions that it will limit advertising and therefore choice of content. We would ask that the final code recognises ways for companies to continue to deliver age appropriate advertising, as long as that is communicated honestly and transparently, to be able to deliver free content for children and their families.

2. Age-appropriate application

Yes

Although the BTHA is aligned on the age appropriateness of the terms and conditions the extension of age from 13+ to 18 may cause issues with integration from the PECR.

Parents overall do not have the time to read and understand the requirements for every new ISS so the BTHA suggests the ICO come up with parent and child formats for specific data areas and host it in a central location for companies to link to. The code will make it too onorous for the majority of parents, leading them to agree to share data because they haven't read the documents, due to consent fatigue, causing the code of practice to be worthless. Making it possible for child users to take off default settings will help to alleviate the burden on parental time but we would also suggest that the ICO give more clarity on this.

If this information were hosted in one portal (with different areas for different ages) companies could link to the messaging which would be consistent and parents and children would begin to understand the various types of data requests to help them make informed choices. This would cut down on the burden to business and help bring understanding through consistency of messaging to parents and children who would get used to the consistent video, audio and written files.

3. Transparency

Yes

Because the Code proposed would apply to practically all users of all websites, the transparency requirements may result in a dramatic increase in pop-ups and other just-in-time notices presented to adults. Those constant interruptions will disrupt the quick-click nature of internet browsing and will likely confuse and annoy the user, rather than encourage thoughtful review of privacy implications and could lead to

users accepting options automatically rather than with considered thought.

4. Detrimental use of data

No

5. Policies and community standards

No

If YES, then please provide your reasons for this view.

6. Default settings

Yes

We have great concern regarding the default being set at the highest privacy setting since it may cause many services to no longer be free and will greatly reduce choice and control of content.

If profiling is turned off by default, it will prevent the free use of many apps and services. We are concerned that if carried out to the letter, this will gut the digital gaming and entertainment industry's entire economic model of advertising revenue for "free" entertainment and/or content. We believe that there is a high risk of a chilling effect industry-wide based on cost to implement and difficult or uncertain standards to meet and ensure compliancy. Ultimately, publishers will opt not to publish in the UK rather than take the steps to comply with all the standards. We understand from our meeting that this is not the intention of the ICO and ask that more consultation is taken on the final text to ensure this consequence has been overcome before the final text is passed.

Although the research which accompanied the code talked about turning settings by default to the highest level there were no questions asked about parents and children understanding the relationship between data capture and free content. If industry concerns are not addressed, the code of practice will lead to a reduction in service and potential loss of free services with a reduction in innovation across the UK, EU and wider areas.

We would suggest that companies are required to be honest, truthful and transparent in making clear requests for data and how it will be used in order to be able to deliver ads that are age appropriate for the age of user of any given ISS. If the information is fairly obtained with correct permissions, we would ask that this be allowable.

Updating the code to make it clear that alterations in settings can be done without age verification by self declaration of the user would be key here.

7. Data minimisation

Yes

We believe this code will lead to consumers believing all data is bad, but in fact there are real benefits to being able to shape an online experience to a user depending on data such as their previous history, gaming level etc. We would ask that the final code balances messaging about the use of data, responsible use and transparency, with the experience it brings and with messaging about data minimisation. Users need to know that the experience they have can be linked to the data they share and it would be useful if the final code from the ICO balanced the messaging around responsible behaviour.

Requiring age verification without accepting self-declaration could result in the collection of additional sensitive information that goes against the principles of data minimisation.

The compliance options set forth in the Code are either to apply standards to all users by default or to offer a robust age-verification mechanism, with a strong recommendation for the latter in order to tailor the experience for each age range. We believe that the collection of data for the purpose of age verification should be proportionate to the data processing activity being contemplated. For example, it would be excessive to require personal information such as payment card details or national ID in order to establish age on a website that collects only limited personal information and uses it only for legitimate interest purposes. While it may be appropriate to collect more information and permissions if information is going to be used for targeted marketing purposes or shared with third parties, the collection of information for age verification should take place consistently with the GDPR principle of proportionality. In some cases, where there is very minimal collection and processing of data, asking a user to self-declare their age may be a sufficient age check and we welcomed the ICO confirmation of this approach when we met. We would welcome more clarification in the final text.

8. Data sharing

Yes

The code should not create a higher standard for sharing data outside of the parameters of the GDPR since it may inadvertantly and inappropriately hinder sharing with processors.

9. Geolocation

Yes

Geofencing is required to provide users with language-appropriate and cultural services. Hard identifiers are not required for this use to work;

only country-city level IP address analysis is needed. Given that an IP address is a standard requirement in the standard transmission of a HTTP header request we would ask that this remain possible and outside the "strongest default" options as the consequence would be to cut down on user overall experience without giving critical data away.

10. Parental controls

Yes

We are concerned that parental controls may have been developed in products to help parents with safety concerns and that those features may now either be disabled or companies will stop using the technology as they will be worried about the regulations surrounding their use. Disabling these safeguards could in fact put children at more risk rather than safeguarding them.

The GDPR's privacy by default requirement does not mean that parental controls must be switched on by default. We would ask that instead the code encourages companies to allow parents to accompany their children through the set up process of a connected toy which will support active choice meaning they engage more on the options available, make family-appropriate choices and talk to and educate their child in the process.

11. Profiling

Yes

Some profiling or personalisation within a given experience should be permissible since the data is integral to the experience, for example, previous gaming history and level.

12. Nudge techniques

No

If YES, then please provide your reasons for this view.

13. Connected toys and devices

Yes

Whilst the toy industry has control over its own services and apps and how they interact with devices, including encryption and security, it has no way of policing platforms such as Amazon (Alexa/Echo) or Google (Cloud) and have no way of accessing the data retrieved by these platforms or how they in turn use the data they collect. We would ask that thought is given to ringfencing business relationships and making clear with which party in a supply chain (at the level of being responsible for the data capture) responsibility lies.

14. Online tools

No

If YES, then please provide your reasons for this view.

15. Data protection impact assessments

Yes

To consult with children and parents for every DPIA is an immense responsibility for toy companies. It would be very costly if every activity they undertook had to be accompanied by a consultation. For example, every website change needs a consultative approach. It is costly, restrictive and not a level playing field for UK companies to compete with other EU and wider companies and may result in UK based companies being less innovative and successful compared to overseas competitors.

Data controllers should be allowed flexibility in deciding the need of a DPIA taking into consideration its context. GDPR requires DPIA when processing is likely to cause a high risk to rights and freedoms of individuals. It should not be taken for granted that all processing of personal data of minors automatically increases to high risk. We believe this may unintentionally impact on the competitiveness of the toy industry with other competitive industires and the UK toy industry with other international industries.

16. Governance and accountability

Yes

The juristiction of the ICO will be the UK. We see unintended consequences in the restriction of practices for legitimate UK companies that will be permissable by default by foreign competitors. UK enforcement is under-resourced already and we see the results in safety compliance. Responsible toy companies invest huge amounts of money to ensure the toys they make comply with the toy safety directive, whilst non compliant and unsafe toys continue to be sold in the UK via online marketplaces. We have been talking to enforcement and regulators for almost a year and the situation has not changed as our enforcement juristiction is limited to the UK and the marketplaces have no mandate to police their own platforms. We are concerned that now regulation will come in on data privacy and the responsible UK based toy companies will invest heavily in this area only to find their competitors are not complying and are not being policed. We would ask that consideration will be given to ensuring that a burden is not being placed on the responsible sector that already consider good practice in this area whilst non reputable companies continue to gain commercial advantage by non-compliance.

In addition, we would ask that parameters are set around data which is in a companies control, and data that is not. Smart

speakers like Amazon Alexa/Echo etc. are different than designing toys for use with mobile devices because with a mobile device, the developer has more control of how the app interacts with the device—and its security and level of encryption. This allows much more precision than when relying on the voice analysis computing that occurs in the Amazon or Google cloud which is out of a toy device developers control. Further, as app or skill developers, we must trust that the entire platform is operating in a compliant manner; we do not have access to the data that's being collected by the system from users (other than aggregated analytics information that the platform provider gives as feedback) and cannot anticipate all the ways that a platform might be connecting data elements together. We would ask for more clarify on the responsibility in the supply chain for data capture versus processing and how that interacts with other connected devices in the home as to the responsibility level of the company.

Q6. Do you envisage any feasibility challenges to online services delivering this standard?

1. **Best interests of the child**
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
2. Age-appropriate application
Yes It is now very unclear how the industry is to make age appropriate content whilst being unable to verify age due to data limits. We understand from meeting you that this is not your intention and therefore ask that this is clarified in the paper to avoid unintended consequences.
3. Transparency
Yes In addition to the issue of verifying the age of users based on the stringent standards of the code, having to provide multiple notices for different audiences will be onerous, impractical and impossible to comply with in the short-term.
4. Detrimental use of data

No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
5. Policies and community standards
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
6. Default settings
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
7. Data minimisation
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
8. Data sharing
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
9. Geolocation
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
10. Parental controls
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
11. Profiling
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
12. Nudge techniques
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
13. Connected toys and devices

No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
14. Online tools
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
15. Data protection impact assessments
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.
16. Governance and accountability
No If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

Q7. Do you think this standard requires a transition period of any longer than 3 months after the code come into force?

1. **Best interests of the child**
No
2. Age-appropriate application
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
3. Transparency
No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
4. Detrimental use of data
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
5. Policies and community standards
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
6. Default settings
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
7. Data minimisation
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why
8. Data sharing
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
9. Geolocation
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
10. Parental controls

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

11. Profiling

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

12. Nudge techniques

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

13. Connected toys and devices

Yes

The code is asking for an icon at point of purchase. This is a reasonable request but will take time to achieve on a physical product - on Page 79 the code lays out the requirements for an icon or information on packaging. This will not be possible in 61 days. Toys take 18 months to 2 years to develop from beginning to market shelf. Clearly new requirements on software will be able to upload as an update, however there should be awareness of timescales for 'hardware' development. Companies will have developed products to the GDPR requirements but will not have seen these current code requirements before. Toys need factory time plus three months shipping at sea meaning that a minimum of 12 months would be needed for toy companies to ensure they have an icon on packaging and hardware requirements (such as the light up when connected) built in.

Changes to design and packaging will also cost companies money as even after the minimum timeframes they will need to rework packaging artwork or toy design. This can of course be done but the longer companies are given to incorporate this into initial designs the less burdensome the changes become.

Many toys are made out of season to be able to meet demand at Christmas. Therefore this Christmas' connected toys are being manufacturered in China in the next month for storage before being shipped to retail from October.

We would ask that changes in this legislation follow other toy safety timelines, for example toy safety standards have a transition period that begin from the moment they are written in as statutes. This allows

companies time to understand and comply with the new requirements and to make the necessary changes without incurring more cost than is necessary and allowing them to communicate any changes that are necessary to both suppliers and their customers. That period is unsually 6 months to one year. We would ask for a year in this case due to the redesign, remodelling and tooling that would be needed in this case for the physical product design.

A separate issue is sell-through of product. Once the new code is published there will be product on the shelves in the UK that is made to comply with the GDPR but again will not have been made to this new requirement. There should be an acceptable sell-through period such as the rules relating to "placed on the market" items under the EU Blue Book definition. This definition will be recognised by both companies and enforcement as it is a tried and tested method that has been used when there are new safety standards.

14. Online tools

Yes

This is a far more complex code than was expected and alters requirements for companies to deliver. The two months suggested is not enough time for companies to assess their systems, conduct DPIA's for all of them, potentially indertake consultations on each one, assess the changes needed, product audio, video and cartoon files, produce parental advice and then add this to every ISS they have up and running as well as those they are developing. We think this is an unfair and unreasonable timeframe and would ask that this legislation follow the timing of other legislative changes by giving a year for transition.

Changes as far ranging as those intended have a considerable impact to mobile game architecture. For software with an existing involved user base, this will present considerable expense and time to design for. For many existing games and apps, we believe that publishers will likely choose to sunset titles that may not be currently driving revenue rather than take on this work. For websites, this also represents a huge amount of volume with a concern that the user experience will be diminished to the extent that there will not be a cost-benefit advantage to keep many sites live.

15. Data protection impact assessments

No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.
16. Governance and accountability
No If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Q8. Do you know of any online resources that you think could be usefully linked to from this section of the code?

1. **Best interests of the child**
No If YES, then please provide details (including links).
2. Age-appropriate application
No If YES, then please provide details (including links).
3. Transparency
No If YES, then please provide details (including links).
4. Detrimental use of data
No If YES, then please provide details (including links).
5. Policies and community standards
No If YES, then please provide details (including links).
6. Default settings

No If YES, then please provide details (including links).
7. Data minimisation
No If YES, then please provide details (including links).
8. Data sharing
No If YES, then please provide details (including links).
9. Geolocation
No If YES, then please provide details (including links).
10. Parental controls
No If YES, then please provide details (including links).
11. Profiling
No If YES, then please provide details (including links).
12. Nudge techniques
No If YES, then please provide details (including links).
13. Connected toys and devices
Yes If YES, then please provide details (including links). BTHA guidance for members of the BTHA can be found at: https://www.btha.co.uk/guidance/connected-toys/
14. Online tools
No If YES, then please provide details (including links).
15. Data protection impact assessments
No If YES, then please provide details (including links).
16. Governance and accountability
No If YES, then please provide details (including links).

Q10. Is the '**Enforcement of this code'** section clearly communicated? Yes If NO, then please provide your reasons for this view.
Q11. Is the '**Glossary'** section of the code clearly communicated? Yes If NO, then please provide your reasons for this view.
Q12. Are there any key terms missing from the '**Glossary'** section? Yes "Compelling Reasons", "Age Appropriate Application" and "Connected Device"
Q13. Is the '**Annex A: Age and developmental stages'** section of the code clearly communicated? Yes If NO, then please provide your reasons for this view.
Q14. Is there any information you think needs to be changed in the '**Annex A: Age and developmental stages**' section of the code? Yes We do not agree with the most common age of a child playing with a connected toy being under the age of 5 years. Please see our attached information showing the ages of the most common connected toys in 2019. This clearly demonstrates the older target age for connected toys.

Q15. Do you know of any online resources that you think could be usefully linked to from **the 'Annex A: Age and developmental stages**' section of the code?

No

If YES, then please provide details (including links).

Q16. Is the **'Annex B: Lawful basis for processing'** section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

Q17. Is this **'Annex C: Data Protection Impact Assessments'** section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

Q18. Do you think any issues raised by the code would benefit from further (post publication) work, research or innovation?

Yes

If YES, then please provide details (including links).

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	☐
A body representing the views or interests of parents? Please specify:	☐
A child development expert? Please specify:	☐
An Academic? Please specify:	☐

An individual acting in another professional capacity? Please specify:	☐
A provider of an ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify: The British Toy and Hobby Association	☒
An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public or a parent)?	☐
An ICO employee?	☐
Other? Please specify:	☐

Thank you for responding to this consultation.

We value your input.