Information Commissioner's Office

Call for evidence:

Age Appropriate Design Code

Start date:27 June 2018
End date: 19 September 2018

ico.
Information Commissioner's Office

V1.0 20180626

Introduction

The Information Commissioner (the Commissioner) is calling for evidence and views on the Age Appropriate Design Code (the Code).

The Code is a requirement of the Data Protection Act 2018 (the Act). The Act supports and supplements the implementation of the EU General Data Protection Regulation (the GDPR).

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. Once it has been published, the Commissioner will be required to take account of any provisions of the Code she considers to be relevant when exercising her regulatory functions. The courts and tribunals will also be required to take account of any provisions they consider to be relevant in proceedings brought before them. The Code may be submitted as evidence in court proceedings.

Further guidance on how the GDPR applies to children's personal data can be found in our guidance Children and the GDPR. It will be useful to read this before responding to the call for evidence, to understand what is already required by the GDPR and what the ICO currently recommends as best practice. In drafting the Code the ICO may consider suggestions that reinforce the specific requirements of the GDPR, or its overarching requirement that children merit special protection, but will disregard any suggestions that fall below this standard.

The Commissioner will be responsible for drafting the Code. The Act provides that the Commissioner must consult with relevant stakeholders when preparing the Code, and submit it to the Secretary of State for Parliamentary approval within 18 months of 25 May 2018. She will publish the Code once it has been approved by Parliament.

This call for evidence is the first stage of the consultation process. The Commissioner seeks evidence and views on the development stages of childhood and age-appropriate design standards for ISS. The Commissioner is particularly interested in evidence based submissions provided by: bodies representing the views of children or parents; child development experts; providers of online services likely to be accessed by children, and trade associations representing such providers. She appreciates that different stakeholders will have different and particular areas of expertise. The Commissioner welcomes responses that are limited to specific areas of interest or expertise and only address questions within these areas, as well as those that address every question

asked. She is not seeking submissions from individual children or parents in this call for evidence as she intends to engage with these stakeholder groups via other dedicated and specifically tailored means.

The Commissioner will use the evidence gathered to inform further work in developing the content of the Code.

The scope of the Code

The Act affords the Commissioner discretion to set such standards of age appropriate design as she considers to be desirable, having regard to the best interests of children, and to provide such guidance as she considers appropriate.

In exercising this discretion the Act requires the Commissioner to have regard to the fact that children have different needs at different ages, and to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

During Parliamentary debate the Government committed to supporting the Commissioner in her development of the Code by providing her with a list of 'minimum standards to be taken into account when designing it.' The Commissioner will have regard to this list both in this call for evidence, and when exercising her discretion to develop such standards as she considers to be desirable

In developing the Code the Commissioner will also take into account that the scope and purpose of the Act, and her role in this respect, is limited to making provision for the processing of personal data.

Responses to this call for evidence must be submitted by 19 September 2018. You can submit your response in one of the following ways:

Online

Download this document and email to:
childrenandtheGDPR@ICO.org.uk

Print off this document and post to:
Age Appropriate Design Code call for evidence
Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

Cheshire SK9 5AF

If you would like further information on the call for evidence please telephone 0303 123 1113 and ask to speak to the Engagement Department about the Age Appropriate Design Code or email childrenandtheGDPR@ICO.org.uk

Privacy statement

For this call for evidence we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our privacy notice.

Section 1: Your views and evidence

Please provide us with your views and evidence in the following areas:

Development needs of children at different ages

The Act requires the Commissioner to take account of the development needs of children at different ages when drafting the Code.

The Commissioner proposes to use their age ranges set out in the report Digital Childhood – addressing childhood development milestones in the Digital Environment as a starting point in this respect. This report draws upon a number of sources including findings of the United Kingdom Council for Child Internet Safety (UKCCIS) Evidence Group in its literature review of Children's online activities risks and safety.

The proposed age ranges are as follows:

3-5
6-9
10-12
13-15
16-17

Q1. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate you consider the above age brackets would be (delete as appropriate):

Not really appropriate

Q1A. Please provide any views or evidence on how appropriate you consider the above age brackets would be in setting design standards for the processing of children's personal data by providers of ISS (online services),

The 5Rights report linked to above provided the basis for the age brackets proposed for the Code. However, on page 10 of that same report the authors also reference designing services with childhood milestones in mind and for this they presented the following age brackets: infancy-5; 6-11; 12-18; and 18-25. Regardless of which age brackets are chosen, many products and services are intended for a broad audience, whether under 18s more broadly or both children and adults. Creating different design standards for different age groups will present a considerable challenge. This may result in additional data collection to determine age, as well as multiple versions of the same products / services to accommodate different age brackets. This will lead to the unintended consequences of organisations

withdrawing products and services from child users and / or an inability for smaller companies to compete with large, established companies, given the additional human and financial resources required to devise and maintain multiple versions of the same product. Therefore, age brackets should be used judiciously to set different design standards in areas where this is appropriate and backed up by evidence indicating different approaches are needed for that particular area, to prevent harm.

As an example, when an organisation designs products and services, and the accompanying user interface and experience, there are several steps to take. Firstly, user research and testing. Secondly, design work and further testing (including user testing) to iterate and improve the design. There can be several rounds of user testing to finalise a design. Thirdly, the building of the feature, product or service. This involves coding and technical expertise and the time required depends on the complexity of what is being built. Fourthly, quality assurance (QA) testing to make sure everything works as it should and has been designed correctly. Finally the feature, product or service is released. This process involves a significant amount of time and so to have to develop different features, products and services for different age brackets would mean going through the above stages for each one separately. As well as the time concern, this would also be a financial burden for many companies who do not have the resource and budget for this approach. This will be particularly acute for start-ups and SMEs and could lead to a lack of competition in the marketplace and a further market consolidation in favour of the larger technology companies.

Q2. Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age brackets.

There has understandably been a lot of focus on social media and games aimed at and used by children, and the impact of marketing and advertising on their development. It is important that any design standards take account of the wide range of products and services aimed at or used by under 18s, so that standards aimed at the social media and games market do not unreasonably adversely impact other services. For example, education or online safety products and services are unlikely to carry out the profiling and marketing activities common to other sectors, and they will collect and use personal information for very different purposes. Products and services that are educational or about increasing online safety are relevant to all ages and it is only the information provided to the user that needs to be tailored according to age.

In addition, the ICO may wish to consider distinguishing between requirements for online services that are 'child-directed' and those that are offered to a 'general audience', which may include under 18s. This would allow the Code to provide for design standards that reflect the service being offered and any associated risks to child users. This is the method adopted by the FTC under the Children's Online Privacy Protection Rule (COPPA). In the context of COPPA, its obligations apply where:

- your website or online service is directed to children [under 13] and you collect personal information from them; or

- your website or online service is directed to children [under 13] and you let others collect personal information from them; or
- your website or online service is directed to a general audience, but you have actual knowledge that you collect personal information from children [under 13]; or
- your company runs an ad network or plug-in, for example, and you have actual knowledge that you collect personal information from users of a website or service directed to children [under 13].

To determine whether a website or online service is 'child directed' the FTC sets out a number of factors to consider. These include "the subject matter of the site or service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children". The FTC will also consider "competent and reliable empirical evidence regarding audience composition, as well as evidence regarding the intended audience of the site or service".

In the context of the Code, elements of the COPPA approach may be helpful, such as applying to child-directed services specific obligations that are aimed at preventing harm to or increasing the privacy levels for children. Some requirements, such as providing alternative versions of T&C or privacy notice, could apply to child-directed services and only to general audience services where they have actual knowledge of child users under a certain age.

The United Nations Convention on the Rights of the Child

The Data Protection Act 2018 requires the Commissioner to take account of the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code.

Q3. Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services)

Article 3 would seem to align with the idea that children's developmental interests should be put before commercial gain. The Code will need to find a balanced approach so that design standards seeking to put children's interests first do not render organisations uncompetitive and unable to operate and grow. This approach may be more feasible for large companies with a pre-existing wide user base but could be significantly restrictive for companies targeting educational or online safety products and services at children.

With regards to the comment above in point c referencing article 36 that suggests it might include aggregating data without consent, the Code should take care to be precise in

requiring design standards on this topic. Aggregation of data takes many forms and is done for many different purposes. Business metrics on users, products and services can be carried out in a way that minimises or does not include identifying personal information, but provides valuable information on performance and issues that drive decision-making with regard to troubleshooting, investment, resource allocation and product development.

Aspects of design

The Government has provided the Commissioner with a list of areas which it proposes she should take into account when drafting the Code.

These are as follows:

- default privacy settings,
- data minimisation standards,
- the presentation and language of terms and conditions and privacy notices,
- uses of geolocation technology,
- automated and semi-automated profiling,
- transparency of paid-for activity such as product placement and marketing,
- the sharing and resale of data,
- the strategies used to encourage extended user engagement,
- user reporting and resolution processes and systems,
- the ability to understand and activate a child's right to erasure, rectification and restriction,
- the ability to access advice from independent, specialist advocates on all data rights, and
- any other aspect of design that the commissioner considers relevant.

Q4. Please provide any views or evidence you think the Commissioner should take into account when explaining the meaning and coverage of these terms in the code.

Default privacy settings: the Code should take care not to interpret this term to mean that every setting that can be adjusted is automatically turned off. Certain default settings are required to make products and services function. Also, it may be the case that certain settings may be appropriate for some age groups and not for others, and so blanket requirements may not be desirable. (This does though present feasibility challenges as set out in the answers to the questions below.)

It has been suggested by some children's groups that settings should revert to the highest-privacy default once a child logs out or navigates away from a service. Depending on the setting and its function this could lead, for example, to a child having to continually change settings every time they log in or use a product / service. Once they have chosen to change a setting, it is a poor user experience to have to activate that setting every single time. To

facilitate such a feature automatically in a product / service would require user tracking of some kind and additional data collection to know they are a user under a certain age.

Data minimisation standards: this is a GDPR requirement so should already be part of an organisation's approach, regardless of whether they have child users of their products / services. It is often the case though that users (of any age) do not necessarily understand the complex technology or operational processes behind the scenes that make the products and services function. Organisations need to connect data minimisation with transparency to explain why the data is necessary, particularly where it is not obvious to the average user, and it is likely that more explanation in simple language is required where users are under 18.

Any requirements of the Code should take into account that it may not be possible to separate out child and adult users. For example, Yoti's architecture is deliberately designed so that all app personal information is held separately and encrypted and Yoti has no access to that data. This is done with the specific intent of safeguarding users and to avoid any possibility of mass surveillance. Without rolling back our privacy protections and tagging data we have no way to identify child users once they have set up an account. (We do have age gating at registration to make sure that users under the relevant digital consent age are blocked until we have a parental consent mechanism in place.)

Once set up, only a user can access their data through their app, which contains the decryption key to bring all their data back together. If a user deletes the app without deleting their account first then they sever the only link to access it, so their data is left floating in our system with no way to access it. Our system deletes all data that has been inactive for 3 years. As Yoti is an identity app, it may be that there are periods of time where a user does not use the app, so because we have no access to the data, we cannot delete inactive data too early, or we risk unilaterally deleting someone's data who just hasn't used the app for a while. Therefore, we would not be able to distinguish inactive child user data from inactive adult user data and apply different retention / deletion periods to the child data.

Presentation and language of terms and conditions: terms contain the obligations on both the user and the company, they form a legal contract and may need to be relied on in court. This is usually why it is challenging to present them in a language and style that children can understand and a court will accept. In explaining terms and conditions in the context of under 18s, the Code should be mindful of the need for terms to protect both parties and for both parties to be able to rely on them in case of a legal challenge. It would be useful if the ICO or children's digital charities could issue a set of educational materials which explain to parents, educators and young people key terms such as liability and third party which in our research young people find challenging.

With regard to the content of terms and what may or may not be appropriate for under 18s, terms for online products and services often contain prohibitions on misusing the product / service; copying content and branding; and technical aspects such as reverse engineering code. Children are increasingly technically competent at younger ages, and technical /

coding skills are increasingly being taught to children, so these are important components of terms that apply to users of all ages.

There has also been criticism of the fact that children can't understand terms, that terms are non-negotiable and that children cannot negotiate their own agreements. This perhaps suggests a misunderstanding of what terms are for. Also, it seems unrealistic and unnecessarily onerous on children to expect them to be able to negotiate terms!

Presentation and language of privacy notices: there has been a lot of debate about the content and presentation of privacy notices generally, and there have been suggestions that they should have a maximum reading age of 13 and a maximum word count. However, greater transparency usually means more words. In reality, explaining complex technology and operational processes and updating privacy information as the products and services expand and develop means that a maximum word count would be completely unworkable. The focus instead should be on clarity of content and presentation, and a layered approach, as recommended by the ICO.

The uses of geolocation technology: the Code needs to be precise in its definition of geolocation technology and consider purpose. 'Location' can mean many things and can be ascertained from many different types of data, and used for many different purposes. Some products and services rely on a location indicator of some kind to function and serve their purpose in a manner that is not privacy intrusive, in other scenarios a location indicator is part of an anti-fraud measure. (For example, an automated identity check at a border checkpoint or age check at a supermarket self-checkout usually requires a location indicator to make sure the person presenting the identity or age credentials is actually present, and not someone else acting remotely.) It should not be the case that the Code interprets location technology as always meaning 'tracking precise locations and movements' and therefore makes it always unacceptable for under 18s.

Automated and semi-automated profiling: the Code needs to be precise in its definition of profiling and consider purpose. 'Profiling' can mean many things and can involve collection and use of many different types of data, and can be used for many different purposes. Some products and services rely on profiling of some kind to function and serve their purpose, in other scenarios profiling is part of an anti-fraud measure. It should not be the case that the Code interprets 'profiling' to always be a negative activity or an activity that leads to targeted advertising. The definition of profiling in GDPR means that it includes, for example, basic data aggregation that is based on unique IDs but that are not accessed, and not able to identify an individual. This is a very different proposition to the collection of multiple data elements to create a user profile to sell to third parties to target advertising.

It is also worth noting that due to the way the mobile advertising ecosystem works a device's advertising identifier (IDFA) is the main data element used.This is also a privacy-protecting measure so that personally identifiable information, such as name, address, date of birth and similar are **not** collected. The controls and settings for that identifier are on the phone and in the user's control. Without additional data collection it is hard to see how organisations can distinguish between IDFAs collected from children and those from adults. It is also impossible to know if a child is using an adult's device. This means that requiring

organisations who offer services to a general audience to prevent children's data from being used for behavioural advertising is impossible to implement.

The sharing and resale of data: the Code needs to be precise about the definition of these terms, given sharing can have may different meanings, and doesn't always mean sale or lead to financial gain. Some products and services have data sharing as an integral part of their function. For example, if you use a password manager, it works by automatically populating your username and password into sites you visit. This could be considered 'data sharing' but is clearly a very different case to organisations selling user data to third parties as a revenue stream.

Suggestions from some children's groups that organisations carry out due diligence on all third parties and remain liable for child personal data after they have shared it with a third party are not only unrealistic, they go against basic concepts of data protection law with regard to data controllers and their obligations and liabilities. As an example, Yoti is a digital identity app and provides an alternative way to prove who you are. Instead of filling in your name and address on a website form, or scanning in a copy of your identity document, a person could share only the required details using Yoti (this is beneficial as the details have been verified so they are also more reliable for the receiving party). It is therefore a disproportionate suggestion that organisations should carry out extensive due diligence on each organisation that might receive data and remain liable for the data the individual chooses to share with the third party. The law already provides for written contracts to be in place between organisations that provide, share or exchange personal data and for those contracts to contain appropriate data protection clauses and guarantees. From a technical perspective, there is no way for an organisation to continue to have access to data that is now held by a third party and to monitor its subsequent use. Having this kind of continued access would also be in breach of GDPR / DPA 2018.

The strategies used to encourage extended user engagement: the Code needs to be precise about the definition of these terms, and focus on where strategies used may cause harm, detriment or adverse impact on under 18s, or a sub-category of under 18s. For example, some products and services remind users where they did not complete a process or to update them on an activity or process. Depending on the activity, service or purpose, it may be in the child's interest to get the reminder or update.

For example, to be able to securely share relevant identity details using Yoti you need to upload an ID document, so you have the details in your account. One of the anti-fraud processes we have in place is to make sure the individual is a real person, and that their account photo matches the ID document photo. If any of these checks fail it is important to alert the user so they can try again, or contact Customer Support. Also, if a user has to stop part way through and later comes back to the app, it is important to alert them that what they were doing has not been completed. This is particularly the case where users try to use the app features but cannot because they haven't completed a check or process.

As already mentioned in other parts of this response, identifying child users to apply different approaches will likely require additional data collection and user tracking of some kind, which is therefore counter productive.

User reporting and resolution processes and systems: most organisations with customer support functions are already able to report on queries received and time taken to resolve them. However, to be able to report on queries and timescales specifically relating to under 18s, or any sub-category of under 18s, will require additional age-related data collection when an individual contacts a company with an issue. If the Code mandates standards in this area, it should be mindful of the differences between user reporting and resolution in the context of social media and online gaming, for example, as compared to the context of educational or online safety services. Any Code requirements on how to deal with with individual rights for child users should align with GDPR / the Data Protection Act 2018. For example, a presumption that any deletion request made an under 18 is automatically valid and should be complied with would undermine the legal requirements for the right and risks deleting information that it is necessary to hold.

Q5. Please provide any views or evidence you have on the following:

Q5A. about the opportunities and challenges you think might arise in setting design standards for the processing of children's personal data by providers of ISS (online services), in each or any of the above areas.

If the Code mandates different designs within products and services for different age groups there is a real danger that start-ups and SMEs will simply be unable to provide services to younger age groups because they do not have the resources to design and build additional products / services. This could have the unintended consequence of increasing the monopoly of large ISS, many of whom have been subject to increasing criticism over their continual failure to act in the best interests of young users of their services.

That notwithstanding, the Code provides an opportunity to set design requirements so that it encourages all organisations (and especially start-ups and SMEs who often do not have a dedicated privacy resource) to consider child users of their services from the start. However, this will require the Code to distinguish between ISS whose services ought to be materially different depending on the age of the user, and those ISS which provide an identical service for all users, no matter what their age.

Q5B. about how the ICO, working with relevant stakeholders, might use the opportunities presented and positively address any challenges you have identified.

As a privacy-focused app which aims to benefit young people and protect young people online, we would welcome the opportunity to speak with the ICO about what is appropriate to mandate and what needs to remain flexible. We would welcome the opportunity to demonstrate some examples of products which could safeguard both younger and older people online, but that it would not be feasible to offer as separate services for small age brackets. Examples include a free password manager; age verification (requiring no more information than that a person is over or under a certain age) for access to age-restricted

social media chat rooms; a reporting tool for under 18s to remove sexting images posted online; a secure door entry system to limit access to a youth centre to only authorised people.

It is important for the ICO to work alongside stakeholders to understand the necessary minimum requirements for the Code to effectively protect under 18s while ensuring that it does not constrain innovation within the sector which could paradoxically help this age group. Further, it will be important for the ICO to engage with stakeholders to ensure that the standards in the Code are not so rigid that it forces organisations to ban under 18 users from using their services.

There are many fora where this discussion could take place. For example, trade organisations such as TechUK already promote the conversation between private and public entities to workshop difficult issues and help develop socially beneficial technologies.

Q5C. about what design standards might be appropriate (ie where the bar should be set) in each or any of the above areas and for each or any of the proposed age brackets.

We have mentioned examples throughout our responses above. We would also reiterate that rather than setting narrow age brackets for all services, we would recommend the Code distinguishes between requirements for online services that are 'child-directed' and those that are offered to a 'general audience', which may include under 18s. This would allow the Code to provide for design standards that reflect the service being offered and any associated risks to child users.

Q5D. examples of ISS design you consider to be good practice.

We think we have designed our app in a way that it is easy to understand and use regardless of your age. We take a plain English approach to text, keep text concise and use icons and animations. We would be happy to share examples of our app screens with you.

Q5E. about any additional areas, not included in the list above that you think should be the subject of a design standard.

Some children's groups have suggested introducing child data protection assessments for any service that might be accessed by a child. The Code should take care to consider the impact on organisations offering services to a general audience (such as education or online safety services) and that this requirement could lead to them carrying out DPIAs on every single thing they do. This would be disproportionate and not in line with the risk-based approach and DPIA requirements in GDPR and the DPA 2018. If the Code mandates certain design standards then organisations building and developing products and services that are directed at children or may be used by them will have to incorporate these design

standards. That obligation plus the legal requirements to carry out DPIAs for high-risk processing would make an additional child-specific DPA redundant.

Q6. If you would be interested in contributing to future solutions focussed work in developing the content of the code please provide the following information. The Commissioner is particularly interested in hearing from bodies representing the views of children or parents, child development experts and trade associations representing providers of online services likely to be accessed by children, in this respect.

Name: [redacted]

Email: [redacted] privacy@yoti.com

Brief summary of what you think you could offer.

Yoti is happy to contribute to the Code's development by providing expertise on how online products and services are designed and built, and the practical impact of any Code requirement on organisations. We are an innovative technology company operating an agile methodology, so we have significant technical expertise. We can therefore provide valuable information on what would be required to implement a Code requirement from a technical, resource and financial perspective.

Further views and evidence

Q7. Please provide any other views or evidence you have that you consider to be relevant to this call for evidence.

Requiring different standards for different age brackets suggests age verification is needed to understand when a product / service is dealing with a particular age bracket. None of the questions though ask about age verification. The Code should be mindful of setting requirements that imply age verification without any further commentary or guidance on how this is to be achieved or what standards are expected.

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:	☐
A provider of ISS likely to be accessed by children? Please specify: Digital identity platform; password manager	☒
A trade association representing ISS providers? Please specify:	☐
An ICO employee?	☐
Other? Please specify:	☐

Thank you for responding to this call for evidence.
We value your input.