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? YES/NO.
Q2. Is the '**Services covered by this code'** section of the code clearly communicated? YES/NO.

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**
YES/NO.
2. Age-appropriate application
No Although it is not explicit, the Code seems to suggest that firms must break down customers into cohorts by age and then apply different protections, privacy notices, etc to each. While this might be suitable in some cases, in other cases it may be appropriate for a firm to apply a single, high level of protection across all relevant customer ages. For example, a firm could design its privacy notices and any 'nudges' to be suitable for mulitiple customer age cohorts. Provided it has tested that these measures are indeed suitable for all applicable cohorts, the firm should be able to apply the same measures and protections. For example, a firm that only accepts customers aged 13 and over should be able to use a privacy notice that is designed for, and tested with, individuals aged 13 and over (subject to ensuring that an appropriate level of detail is available so that important information is not 'hidden' as flagged on page 31). The Code should more explicitly recognise that this approach is acceptable.
3. Transparency
No See comments in relation to 2 - age appropriate design. In addition, it is not clear how to interpret the expectation that information should be provided in multiple formats, such as in writing, audio and video. This could be interpreted as meaning that all three options should be provided for the initial privacy notice, secondary layers, consents AND any just-in-time notifications. We presume that the intention is rather that the firm should consider the most appropriate medium(s) for each and implement those that are appropriate in the context. This should be clarified.
4. Detrimental use of data
YES/NO.

5. Policies and community standards

YES/NO.

6. Default settings

No

On page 43 it should be made clearer that 'high privacy' settings are required for children's settings by default, not all users'. We suggest amending as follows: "Your default position for each individual privacy setting FOR CHILDREN'S SERVICES should be privacy enhancing or 'high privacy'."

On page 46 it should be made more explicit that a customer adjusting a default setting to activate additional data processing does not necessarily mean that this processing is based on 'consent'.

7. Data minimisation

YES/NO.

8. Data sharing

YES/NO.

9. Geolocation

YES/NO.

10. Parental controls

No

See comments above under Question 2: Age appropriate design.

11. Profiling

YES/NO.

12. Nudge techniques

No

See comments above under Question 2: Age appropriate design.

13. Connected toys and devices

YES/NO.
14. Online tools
No See comments above under Question 2: Age appropriate design.
15. Data protection impact assessments
YES/NO.
16. Governance and accountability
YES/NO.

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**
YES/NO.
2. Age-appropriate application
YES/NO.
3. Transparency
YES/NO.
4. Detrimental use of data
YES/NO.
5. Policies and community standards
YES/NO.
6. Default settings:

Yes

It would be helpful to use the example of financial services firms processing and sharing personal data in order to comply with regulation and detect / prevent economic crime. This could include for example monitoring interactions with the customer to meet FCA requirements to 'treat customers fairly', analysing transactions to detect fraud, sending 'suspicious transaction reports' to law enforcement and sharing information about customer fraud with fraud prevention organisations / databases.

We note that children can be taken advantage of by criminals. For example, children can be at risk of being targeted by money launderers to act as 'money mules'.

This is a good example of a clear 'compelling reason' for additional processing.

7. Data minimisation

YES/NO.

8. Data sharing

Yes

Building on the example of preventing online grooming, another good example would be sharing of children's data personal data in order to comply with regulation and detect / prevent economic crime. This could include for example monitoring interactions with the customer to meet FCA requirements to 'treat customers fairly', analysing transactions to detect fraud, sending 'suspicious transaction reports' to law enforcement and sharing information about customer fraud with fraud prevention organisations / databases.

9. Geolocation

Yes

Customer location is an important input into fraud prevention measures used by financial services firms. This would be a helpful example of a 'compelling reason' for geolocation to be active by default.

Further to this, the Code should clarify that in such situations the firm does not need to allow the customer to deactive geolocation, as this would leave customers and firms more vulnerable to fraud. See also comments under Question 5, below.

10. Parental controls

YES/NO.

11. Profiling

Yes Financial services firms use profiling to help them meet regulatory obligations, particularly to detect and prevent fraud and other economic crime. Deactivating this would leave the firm and customers at greater risk. This is good example of a 'compelling reason' to use profiling without giving customers the option of turning it off.
12. Nudge techniques
No
13. Connected toys and devices
YES/NO.
14. Online tools
YES/NO.
15. Data protection impact assessments
YES/NO.
16. Governance and accountability
YES/NO.

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

1. **Best interests of the child**
YES/NO.
2. Age-appropriate application
Yes

Towards the bottom of page 24 the draft Code states "You must not use data collected for age-verification purposes for any other purpose." This is stricter than the GDPR rules, which allow multiple purposes, provided these have a suitable basis for processing and meet other requirements. Financial services firms have regulatory obligations to verify the identity of their customers. This will normally include obtaining the date of birth of the customer from a reliable source such as a passport. This information verifies the age of the customer, potentially to assist with compliance with this Code, but is also necessary for compliance with a range of other legitimate business and regulatory purposes. These include confirming the customer's identity to prevent fraud or money laundering.

It is important that the Code recognise that firms can continue to use age data for other legitimate purposes.

With regards to age verification techniques, we note that on page 25 the ICO commits to working with industry to develop appropriate mechanisms. We agree with this approach. Although not recommended in the Code, we note that in the past in other contexts there has been interest use of credit cards as an age verification tool. We recommend against this, as:
- Children can also make use of parents' or others' credit cards, and are perhaps more inclined to do so when no charge will in fact be made against the card, as could well be the case when the purpose is simply age verification.
- If consumers become accustomed to the idea that they must use a credit card to demonstrate their age, this will make it easier for criminals to successfully set up fraudulent websites and acquire consumers' credentials, facilitating impersonation and fraud.
- Though under-18s cannot be held to a credit card agreement, they can be authorised users on another primacy credit card holder's account. (We note that this is not known practice among UK issuers but can apply to international cards).

3. Transparency

YES/NO.

4. Detrimental use of data

YES/NO.

5. Policies and community standards

YES/NO.

6. Default settings

YES/NO.

7. Data minimisation

Yes

Unlike other sections (eg: 6, 9, 11…), section 7 does not acknowledge that a firm might have compelling reasons for collecting and processing personal data beyond the minimum necessary for 'core service'. As set out under Question 4(6), financial services firms must process personal data for crime prevention and other regulatory purposes.

We presume that it is not intended for part 7 of the Code to prevent this collection / processing; this should be clarified.

8. Data sharing

YES/NO.

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

9. Geolocation

Yes

See comments above under Question 4(9).

Further to this, we query whether it will be in customers' interests to continuously indicate that geolocation is active, when this is for the purposes of regulatory compliance (eg: fraud protection). This might be confusing for customers, given that it cannot be turned off.

10. Parental controls

YES/NO.

11. Profiling

YES/NO.

12. Nudge techniques

YES/NO.

13. Connected toys and devices

YES/NO.

14. Online tools

Yes

Financial services firms have extensive obligations to retain and process personal data for compliance purposes, such as the detection and prevention of money laundering, fraud and other economic crime. In

order to comply with these obligations, they will often need to refuse customers that invoke their rights to object to processing, to have data erased, to have processing restricted, etc. Firms do so in reliance on the exemptions provided under chapter 3 of the GDPR or under those in Schedule 2 of the DPA 2018.

Some customers already misunderstand their right to block processing and secure data erasure, thinking that these rights are absolute in nature. For example, firms have had customers try to object to 'all data sharing', despite firms' need to share with authorities and fraud prevention organisations in order to meet regulatory obligations to detect and prevent crime. The firm then has to explain a complex situation to the customer and explain why it is not possible to follow the customer's request.

There is a risk that providing prominent tools for some rights could lead customers into thinking that they can freely prevent any kind of data processing or can have all of their data erased at will. Given that firms will seldom be able to comply with such requests, this will likely lead to customer confusion and dissatisfaction.

In the financial services context, more focused tools to facilitate Data Subject Access Requests, rectification, data portability and objections to marketing would often be appropriate. However, tools in relation to rights to erasure, to object, to restrict and in relation to automated decisions would risk causing customer confusion.

The Code should allow firms flexibility to determine which kinds of tools are suitable in the context of their services and other legal / regulatory obligations.

15. Data protection impact assessments

YES/NO.

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

16. Governance and accountability

YES/NO.

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

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

1. **Best interests of the child**

Yes

Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
2. Age-appropriate application
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
3. Transparency
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
4. Detrimental use of data
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
5. Policies and community standards
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
6. Default settings
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
7. Data minimisation
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
8. Data sharing
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
9. Geolocation
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
10. Parental controls

Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
11. Profiling
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
12. Nudge techniques
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
13. Connected toys and devices
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
14. Online tools
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
15. Data protection impact assessments
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.
16. Governance and accountability
Yes Please see our overarching comments relating to the wider regulatory environment that financial services firms operate in.

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**

Yes

Three months would be a very tight timeframe for firms to implement the Code. This is because:
- Financial services firms operate in a complex and stringent regulatory environment governed by FCA rules. Please see our overarching comments made at the beginning of our response.
- In designing protection measures for children to date, many firms have concentrated on the age threshold of 13 in the Data Protection Act.
- Implementing the code will require:

i. Identification of impacted services and products (likely to include online and mobile banking services / apps available to customers aged under 18, and potentially some website services)
ii. Analysis of how that product sits relative to each of the 16 standards
iii. Analysis of interactions with other regulatory requirements
iv. Review and update of DPIAs
v. Designing changes to meet the 16 standards, while still complying with the extensive other requirements imposed by the FCA, including potentially different settings for different age groups. This requires input from across the business, including legal and privacy teams, product design and customer experience, and IT.
vi. Implementing the technical changes to give effect to the product changes; firms cannot necessarily do this at will, needing to wait for an appropriate window in which updates can be rolled out.
vii. Internal policies and procedures will also need to be updated to incorporate the new standards.

This review and implementation process will likely take 12 or even 18 months.

2. Age-appropriate application

Yes

See comments above under 1. Best interests of the child

3. Transparency

Yes

See comments above under 1. Best interests of the child

4. Detrimental use of data
Yes See comments above under 1. Best interests of the child
5. Policies and community standards
Yes See comments above under 1. Best interests of the child
6. Default settings
Yes See comments above under 1. Best interests of the child
7. Data minimisation
Yes See comments above under 1. Best interests of the child
8. Data sharing
Yes See comments above under 1. Best interests of the child
9. Geolocation
Yes See comments above under 1. Best interests of the child
10. Parental controls
Yes See comments above under 1. Best interests of the child
11. Profiling
Yes See comments above under 1. Best interests of the child
12. Nudge techniques
Yes See comments above under 1. Best interests of the child
13. Connected toys and devices
Yes See comments above under 1. Best interests of the child

14. Online tools
Yes See comments above under 1. Best interests of the child
15. Data protection impact assessments
Yes See comments above under 1. Best interests of the child
16. Governance and accountability
Yes See comments above under 1. Best interests of the child

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**
YES/NO.
2. Age-appropriate application
YES/NO.
3. Transparency
YES/NO.
4. Detrimental use of data
YES/NO.
5. Policies and community standards
YES/NO.

6. Default settings
YES/NO.
7. Data minimisation
YES/NO.
8. Data sharing
YES/NO.
9. Geolocation
YES/NO.
10. Parental controls
YES/NO.
11. Profiling
YES/NO.
12. Nudge techniques
Yes
13. Connected toys and devices
No
14. Online tools
YES/NO.
15. Data protection impact assessments
YES/NO.
16. Governance and accountability
YES/NO.

Q9. Is the '**Enforcement of this code'** section clearly communicated? YES/NO.
Q10. Is the '**Glossary'** section of the code clearly communicated? YES/NO.
Q11. Are there any key terms missing from the '**Glossary'** section? YES/NO.
Q12. Is the '**Annex A: Age and developmental stages'** section of the code clearly communicated? YES/NO.
Q13. Is there any information you think needs to be changed in the '**Annex A: Age and developmental stages**' section of the code? YES/NO.
Q14. 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? YES/NO.

Q15. Is the **'Annex B: Lawful basis for processing'** section of the code clearly communicated? YES/NO.
Q16. Is this **'Annex C: Data Protection Impact Assessments'** section of the code clearly communicated? YES/NO.
Q17. Do you think any issues raised by the code would benefit from further (post publication) work, research or innovation? YES/NO.

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: UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation. If you have any questions in relation to this response, please contact Walter McCahon, Manager: Data Policy, at [redacted]	☒
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.