ICO Age Appropriate Design Code Enters Into Force

Date : September 2, 2020

Introduction

The Information Commissioner's Office ("ICO")'s "Age Appropriate Design Code" ("the Code") is now in force, i.e. as from 2 September 2020. This statutory code of practice is not new law – instead it sets standards and explains how data protection rules apply in the context of children using digital services (mainly the EU General Data Protection Regulation [GDPR] and to a lesser extent the UK Privacy and Electronic Communications Regulations [PECR]). This article highlights key aspects of the Code.

What's this all about?

As the ICO puts it, "[o]ne in five UK internet users are children, but they are using an internet that was not designed for them". Further, children are being "datafied" through organisations recording a mass of data points about them as they grow up including "details about their mood and their friendships to what time they woke up and when they went to bed".

The aim of the Code is to address risks in the use of children's personal data by online service providers through adherence to fifteen flexible standards. Children warrant special protection and so conforming to the Code should ensure that the best interests of the child are taken into account.

The standards are of "age appropriate design" (hence the name of the Code) reflecting a risk-based approach. The focus is on providing default settings which ensures that children have the best possible access to online services while minimising data collection and use, by default. It also ensures that children who choose to change their default settings get the right information, guidance and advice before they do so along with proper protection in how their data is used afterwards.

The standards are cumulative and interlinked and must all be implemented in order to demonstrate conformity with the Code (to the extent that they are relevant to the service in question) and are a key measure of compliance with data protection legislation.

What goods and services does the Code apply to?

The Code applies to "information society services likely to be accessed by children" in the UK – the ICO considers that "for a service to be 'likely' to be accessed, the possibility of this happening needs to be more probable than not". Many apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet therefore fall in scope. According to the ICO, "[t]he vast majority of online services used by children are covered", subject to some limited exceptions e.g. websites or apps specifically offering online counselling or other preventive services (such as health screenings or check-ups) to children. Note that the Code is not restricted to services specifically directed at children.

What are the standards?

The fifteen standards are as follows:

- The best interests of the child – these are the primary consideration when designing and developing online services "likely to be accessed" by a child. Consider the needs of child users and work out how to best support those needs in the design of an online service when processing their personal data. In doing this take into account the age of the user. Evidence and advice from expert third parties may be needed to help do this;
- Data Protection Impact Assessments (a DPIA) – a DPIA should be undertaken in order to assess and mitigate risks to the rights and freedoms of children who are likely to access a service. This should take into

account differing ages, capacities and development needs and builds in compliance with the Code. A DPIA should also consider broader risks to the rights and freedoms of children that might arise from processing their personal data, including the potential for any significant material, physical, psychological or social harm. A template DPIA is provided in the Code;

- Age appropriate application – this means that the age range of the audience and the different needs of children at different ages and stages of development should be at the heart of how the online service is defined and the Code is applied. A risk-based approach should be undertaken in order to recognise the age of individual users and to ensure the Code standards are effectively applied to child users. In practice this means: either, establishing age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from the data processing in question; or, applying the Code the standards to all users. Various tools can be used to establish age, e.g. third party age verification services;
- Transparency – the privacy information provided to users, along with other published terms, policies and community standards, should be concise, prominent and in clear language suited to the age of a child. Additional specific “bite-sized” explanations about how the personal data is used at the point that use is activated should also be provided. The Code provides a table with some transparency recommendations according to age-range;
- Detrimental use of data – children’s personal data should not be used 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. Take particular care when profiling children, including making inferences based on their personal data, or processing geo-location data. Designing in data-driven features which make it difficult for children to disengage with an online service is likely to breach the GDPR fairness principle, e.g. features which use personal data to exploit human susceptibility to reward, anticipatory and pleasure seeking behaviours, or peer pressure;
- Policies and community standards – published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies) should all be upheld. When children provide their personal data in order to join or access an online service they should be able to expect the service to operate in the way that the provider says it will, and for the provider to do what it says it is going to do, otherwise collection of children’s personal data may breach the GDPR fairness principle;
- Default settings – settings should be at a “high privacy” level by default, unless a compelling reason for a different default setting which takes into account of the best interests of the child can be set. Further, by default, a provider should not: collect any more personal data than needed to provide each individual element of the online service; or, make users’ personal data visible to indefinite numbers of other users of the online service;
- Data minimization – only the minimum amount of personal data needed to provide the elements of the online service in which a child is actively and knowingly engaged should be collected and retained. Children should be given separate choices over which elements they wish to activate. There should be no “bundling in” of the collection of children’s personal data in order to provide enhancements of users’ online experience with the collection of personal data needed to provide the core service as this is in effect collecting personal data for different purposes and in breach of the GPR purpose limitation principle;
- Data sharing – sharing children’s personal data with third parties, including sharing data inferred or derived from their personal data, can expose children to risks arising from their processing of personal data, which go beyond those inherent in processing for the service. Therefore, disclosing children’s data should not be shared unless a compelling reason for doing so can be shown, which takes into account the best interests of the child, e.g. data sharing for safeguarding purposes, preventing child sexual exploitation and abuse online, or for the purposes of preventing or detecting crimes against children such as online grooming; an example that is unlikely to amount to a compelling reason for data sharing is selling on children’s personal data for commercial re-use;
- Geolocation – The use of geolocation data in relation to children is of particular concern because the ability to ascertain or track the physical location of a child carries with it the risk that the data could be misused to compromise the physical safety of that child. Geolocation options by default should be switched off, unless a compelling reason for geolocation to be switched on by default can be shown, which takes into account the best interests of the child, e.g. it may be possible to argue that metrics needed to measure demand for regional services may be sufficiently un-intrusive to be warranted (taking into account the best interests of the child). An obvious sign for children when location tracking is active should be provided. Options which make a child’s location visible to others must default back to “off” at the end of each session;

- Parental controls – Parental controls are tools which allow parents or guardians to place limits on a child's online activity and thereby mitigate the risks that the child might be exposed to, e.g. restricting internet access to pre-approved sites only and restricting in-app purchases. They can also be used to monitor a child's online activity or to track their physical location. Whilst these controls are important they may also impact on the child's right to privacy. Where parental controls are provided the child should be provided with age appropriate information about this. If an online service allows a parent or a carer to monitor their child's online activity or track their location an obvious sign should be provided to the child when they are being monitored. The Code provides a table with some recommendations according to age-range about the type of information which might be provided and how to provide it;
- Profiling – switch options which use profiling "off" by default, unless a compelling reason for profiling to be on by default can be shown, which takes into account the best interests of the child. Profiling should only be allowed where there are 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. If cookies are used for the purposes of profiling the PECR rules for the setting of the cookie will need to be considered, along with GDPR and the Code for the underlying processing of personal data (profiling) that the cookie supports or enables;
- Nudge techniques – nudge techniques are design features which lead or encourage users to follow the designer's preferred paths in the user's decision making. Nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections should not be used. There should be no exploitation of unconscious psychological processes to this end (such as associations between certain colours or imagery and positive outcomes, or human affirmation needs). Nor should there be use of nudge techniques that might lead children to lie about their age, e.g. pre-selecting an older age range for them, or not allowing them the option of selecting their true age range. Nudging can also be done in a pro-privacy way. The Code provides a table with some recommendations according to age-range about the type of information which might be provided and how to provide it concerning nudging to promote health and wellbeing;
- Connected toys and devices (i.e. where they are connected to the internet) – where a connected toy or device is provided which collects personal data and transmits it via a network connection it must conform to the standards of the Code, e.g. be clear about who will process the personal data that the device transmits via the network connection and what their data protection responsibilities are. Provide clear information about the use of personal data at point of purchase and on set-up. Also avoid the passive collection of personal data such as by providing features that make it clear to the child or their parent when personal data is being collected, e.g. a light that switches on when the device is audio recording or filming; and,
- Online tools – there is an obligation not just to allow children to exercise their rights but to help them to do so. Prominent and accessible tools to help children exercise their data protection rights and report concerns should therefore be provided. The Code provides a table with some recommendations according to age-range about the types of tools that could be used.

The ICO says that "[t]he standards are not intended as technical standards, but as a set of technology-neutral design principles and practical privacy features. The focus of the code is to set a benchmark for the appropriate protection of children's personal data. Different services will require different technical solutions".

What is the legal status of the Code?

The ICO says that it "must take the code into account when considering whether an online service has complied with its data protection obligations under the GDPR or PECR". Further, "[t]he code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant". The ICO also says that "[i]n accordance with our Regulatory Action Policy, when considering any enforcement action we will take into account the efforts you have made towards conformance during the transition period, as well as the size and resources of your organisation, and the risks to children inherent in your data processing. […] If you don't conform to the standards in this code, you are likely to find it more difficult to demonstrate that your processing is fair and complies with the GDPR and PECR. If you process a child's personal data in breach of the GDPR or PECR, we can take action against you".

Are there any sanctions for non-compliance with the Code?

Organisations that do not follow the Code could face enforcement action by the ICO, which includes compulsory audits (which the ICO says it will undertake proactively), orders to stop processing and fines of up to 4% of global turnover.

Do I have to make any changes?

Possibly, depending on your situation. Any changes must be completed by 2 September 2021, which is the date from when the ICO will have to take the Code into account "when considering whether an online service has complied with its data protection obligations" under both GDPR and PECR. The ICO encourages businesses to comply as soon as possible with the new requirements as the Code will apply to both new and existing services. Efforts made to comply during the transition period will be taken into account by the ICO when considering any enforcement action after 2 September 2021.

Do disabilities have to be factored in?

Children with disabilities may have additional needs and so service providers should also consider any additional responsibilities they may have under the applicable UK equality legislation.

Do I have to demonstrate compliance with the Code?

Yes. According to the ICO, systems should be put in place to support and demonstrate compliance with the Code (and data protection legislation) which should include implementing an accountability programme, having suitable data protection policies in place, providing appropriate training for staff and keeping proper records of processing activities.

Is there a transition phase?

Yes, there is a transition period of 12 months in order to give online services time to conform. According to the ICO, "Our approach is to encourage conformance and we would encourage you to start preparing for the code taking effect sooner rather than later."

What about Brexit?

Whether the UK leaves the EU with or without a deal the Code will continue to apply. If there is no deal a UK version of GDPR will be adopted, which the Code will sit alongside, and if there is a deal there will be an implementation period during which GDPR and the Code will continue to apply in the UK after which a UK version of GDPR will apply that the Code will sit with.

What are the takeaways?

Businesses should consider doing the following:

- Reviewing the business' existing online services to establish whether they are covered – the Code provides a flow chart to help determine this;
- For services that are covered, either review your existing DPIA or do a new one;
- Where changes include changes to physical rather than purely online products make sure that the necessary changes are incorporated into manufacturing cycles schedules commencing after 2 September 2021, e.g. for changes to packaging or the physical component of a connected toy – there will not be a requirement to recall or amend existing stock or to amend manufacturing cycles that were already scheduled to commence before 2 September 2021 (when the Code came into force);
- Address how to manage any changes to the way in which a service operates with existing users; and,
- Make any changes to the service as soon as possible – at the very least by 2 September 2021.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For information about our Breach Navigator tool please see here: https://www.corderycompliance.com/solutions/breach-navigator/

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/.

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/

and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

The ICO's Age Appropriate Design Code can be found here https://ico.org.uk/media/about-the-ico/documents/2618093/code-of-practice-dpa-2018-age-appropriate-design-code_v_2_1.pdf

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com