The Age Appropriate Design Code

5Rights Foundation briefing
January 2020

Overview

The Age Appropriate Design Code ('the Code') is the first of its kind anywhere in the world. It is a statutory code of practice setting out the specific protections that children and young people require for their data, offering a much higher level of privacy protection by default. Data is the driving force behind many norms of the digital world, and the way children's data is collected, shared, and used impacts significantly not just on their digital experience, but also on their wider lives. As such, the Code offers a significant and welcome change in how children and young people are protected and supported in the digital age.

The Information Commissioner's Office (ICO) is responsible for implementing and enforcing the Code. Following a consultation on a draft version (April 2019), the ICO has now published an updated and final version of the Code.

About the Code

The Code contains 15 'provisions' relating to children's data protection, representing a sea change in industry norms that will radically improve children and young people's experiences online. It provides protection to **all children under 18** and applies to all services **'likely to be accessed by children'**. Highlights include:

- ***'The best interests of the child should be a primary consideration when you design and develop online services**.'* This is the overarching requirement of the Code and is a well-established legal principle. While individual cases may be complex, it will generally serve to prioritise children's interests above commercial interests.
- Compliance with the Code will be demonstrated by **Data Impact Assessments** specific to children. This demands that companies *'identify and fix problems at an early stage, designing data protection in from the start.'*
- The Code makes services **accountable for how well they uphold their own polices and community standards**, and establishes this as a fundamental precondition of fairness under GDPR. In other words, if you don't provide children with the environment you say you will, the processing of data can't be 'fair' or 'transparent'.
- The Code makes services **responsible for the recommendations they make to children on the basis of their personal data**. Steps must be taken to avoid recommendations '*that are obviously, or have shown to be, detrimental to their health or wellbeing'* (such as recommending self-harm or suicide content).
- **Profiling for the purposes of behavioural advertising** must be off by default for children. If switched on, services are responsible for the advertising they serve to children, as above.
- The Code requires services to provide a **clear indication to children whenever they are processing or broadcasting geolocation data.**
- **'Nudge' techniques** that encourage children to activate low-privacy settings, or to make it harder for them to activate high-privacy settings, are ruled out by the Code.

- The Code challenges the **passive collection of data by connected devices,** and **'inferred data'** is explicitly covered by the Code, which is an important and necessary clarification.

The Code's requirements are proportionate to the risks arising from a service's processing of data. Services that process limited amounts of data for limited and defined purposes will find the code proportional to their processing, services that process huge amounts of data, share it widely, or use it to make complex and impactful decisions about users will have more to do.

The Code is derived from GDPR principles, including data minimisation, purpose limitation, and data protection by design and default. As such, it is 'ready baked' for adoption by States and institutions that are already GDPR compliant.

Age assurance

The biggest difference between the draft version and the final Code relates to the steps that services must take to establish the age of users. The Code now requires services to establish the age of their users to a level of certainty that is appropriate given the risks arising from their data processing. The 'riskier' the processing of user data, the more robust the age assurance needs to be – where risk is indicated by factors including: '*the types of data collected; the volume of data; the intrusiveness of any profiling; whether decision making or other actions follow from profiling; and whether the data is being shared with third parties.'*

The ICO has responded to sector requests for more flexibility and the Code is '*not prescriptive about exactly what methods you should use to establish age'*. Rather, services should be ready to demonstrate through their Data Protection Impact Assessment the steps they have taken to establish the age of users or, where they have not, what measures they have put in place to make their service Code-complaint.

Self-declaration mechanisms are also permissible under the Code, although because self-declaration is not a particularly robust method of age assurance, the Code states that it will only be *'suitable for low risk processing or when used in conjunction with other techniques.'*

Next steps

As per the EU's Directive 2015/1535, the Government is required to notify the European Commission about the Code and abide by a three-month 'standstill' period before bringing it into law.

After that process is complete, the Data Protection Act 2018 requires the Secretary of State to lay the Code in Parliament 'as soon as reasonably practicable'. The Code is subject to the 'negative procedure', which means that it will automatically become law unless a motion to reject it is passed in either House within 40 sitting days (this is very rare). Once it becomes law, a transition period of 12 months will follow in order to give industry enough time to comply with the Code's provisions.

For further information, please read 5Rights' FAQs on the Code. To discuss the Code in more detail, please contact Jay Harman on 02075023818 or jay@5Rightsfoundation.com.