USE YOUR INNER 'BIG' CHILD TO IMPLEMENT THE AGE APPROPRIATE DESIGN CODE

29 / 09 / 2021

Thinking about how to implement the Age Appropriate Design Code issued by the UK's Information Commissioner's Office? Reach out to your inner child!

In the movie Big, Tom Hanks played a child who turned adult overnight. Suddenly, he was in charge of designing toys and he was rather good at it. Unlike the movie, the Code is not a fictional comedy –but perhaps it foretold the approach needed here. Finding your inner child might get you in the right mindset for appreciating the safeguards needed for children of each age group.

The Code's 15 standards mandate, among other things, privacy by default, age verification, targeted geo-location features and discourage disproportionate profiling and nudge techniques which could influence children to their detriment.

Code now in effect

The code became mandatory on 2 September 2021 and the ICO will take it into account in enforcement action.

Each organisation must be able to explain its risk assessment and implementation of appropriate measures or why no measures were taken.

Overarching objective

Children's data must be processed fairly respecting children's best interest. Children must be supported in exercising their basic rights, including the right to play and engage in recreational activities appropriate to their age, and protected from harms such as exploitation. Products and services must be appropriate and meet children's development needs. Pursuing your commercial interests is not prohibited but the best interest of the child must be the primary consideration.

The Code overlaps with the Online Harms Bill which aims to improve UK citizens' safety online by moderating content, monitoring and taking down illegal and harmful content. Conversely, the Code is not intended to moderate content but may still have an indirect impact on it.

Who does the Code apply to?

The Code applies to information society services providers around the world who process the personal data of children in the UK. This includes any online services and connected products, with social media, market places, search engines and connected toys being the usual suspects.

The Code applies only if the services are likely to be accessed by children under the age of 18 in the UK. Even if not aimed at children, your services could be in scope. However, if you determine that the risk is low, minimal safeguards may suffice to comply with the Code. For example, the ICO considers digital news media is not a core concern for children online.[1]

Key steps

Step 1 – Are children likely to access your products and services? Look at your stats and evidence on user behaviour, conduct surveys and map your audiences. It will likely not suffice just including a statement like this without doing further homework: "*We do not knowingly collect, use or share any personal information about children ... without verifiable parental consent .... If you ... believe your child has provided ... information, you can ... request ... information to be deleted ....*" (Stadia).[2]

Step 2 – What are the risks to children? Are they capable of understanding how their data is processed? Larger organisations will be expected to carry out consultations with their audiences, the public and third sector. A DPIA may be required and experts will advise on the likely risks for each age group.

Judge cautiously if your services may raise the risk of exploitation, health risk, emotional harm, social anxiety, bullying, harmful content, misinformation, suppressing one's own views and identity, compulsion, undermining authority, excessive risk-taking, excessive screen time or economic pressure.

Step 3 – What changes are required to your UI, service features and product development to best support children's needs? Turning into a gullible inexperienced child will remind you of the daily perils children face which increase and multiply online. The Code requires you to anticipate these needs like a parent. Privacy by default is a good start but there is so much more.

How is the Code implemented?

Compliance with the Code is likely to affect various aspects of your services. All 15 principles must be complied with at all times and there is no prescribed way of doing so. Your working groups should monitor best practice in the market.

Age verification

The level of risk will dictate how precise your age verification must be. Interrogating your stats may suffice if risk is low. For example, the ICO considers that the risk for news media is low and verifying each user may not be necessary.[3] If risk is high, you may have to ask each user to declare their age or submit to verification by a third party provider or parent. AI verification can be used to increase your age confidence.

On the other hand, Spotify Kids[4], YouTube Kids[5] and PlayStation Now[6] require a parent to set up and regulate the child's account. The Irish DPC has recently started investigating Instagram[7] and TikTok[8] in relation to age verification. Instagram will now lockout users who fail to provide their birthday and AI will be deployed to estimate age from user behaviour.[9]

Transparency

The Code recommends concise, prominent transparency messaging in clear language suited to the age of the child. This should be accompanied by additional 'bite-sized' explanations at the relevant point. You cannot rely on the child or parent seeking out the information.

Legal text should be mirrored by child-friendly explanations. For lower ages, videos, graphics, sounds and other features can be used to make the privacy notice more appealing. However, separate child-friendly notices may not be required for low risk industries, such as news media.[10]

Resources should be provided for children and parents. TikTok was recently fined for not providing a privacy notice in local language.[11]

User choice

Without choices, parents may decide not to allow the service depriving the child of any beneficial activities. In response, organisations have introduced new choices but also taken choices away.

Implementing privacy by default will enable children to take action when they are ready and just-in-time notices will helpfully remind them about the consequences of turning on a feature.

TikTok has recently disabled messaging features for under 16s and their content cannot be downloaded.[12] New content sharing choices and warnings are presented when publishing one's first video. YouTube will remind users about who has access to their content.[13] GEForce Now prevents under 13s from participating in user forums.[14]

Nudge techniques

Encouraging children to stay online can have a serious impact on them. Nudge techniques must not be used to encourage children to provide unnecessary personal data or erode their privacy settings.

TikTok has recently disabled push notification for 13-15s after 9pm and for 16-17s after 10pm. YouTube will turn on **its "take a break" and bedtime reminders** for all users aged 13 to 17 and will turn off autoplay.[15]

Content

The Code does not regulate content. However, it does regulate the use of personal data to suggest content, particularly content that could encourage excessive consumption or cause other harms.

YouTube will remove "unboxing videos", content that "incites viewers to buy a product" and "content focused on the excessive accumulation or consumption of products".[16]

Google's SafeSearch filtering technology will restrict access to adult content for under 13s.

Location data

Unless there is a compelling reason, geolocation tracking must be switched off. Signage must alert the child when it is on. Sharing location with others must be switched off at the end of each session.

Google is planning to turn off all location history for all under 18s globally.

Rights

Children must be presented with prominent tools to exercise their data rights.

Google will allow under 18s or a parent or guardian to request the removal of their images from Google Image search results.

Parental oversight

The Code does not allow invisible monitoring by parents. Instead, signage must indicate when the account is monitored.

Monetisation

While not prohibited, data sharing will only be permitted if there is a compelling reason to do so, taking account of the child's best interest.

This will significantly affect an organisation's ability to sell data. However, sharing data in the context of commercial partnerships where the outcome is beneficial for the child may be appropriate.

Hardware conformity

Any connected toys and devices must also comply with the Code.

Profiling and behavioural advertising

The Code will not prevent organisations from using behavioural advertising which the ICO recognises is an important income stream.

However, such advertising must comply with regulatory codes such as those of the Advertising Standards Authority which protect children. If based on cookies, advertising must be off by default for child users. Profiling must be controlled by safeguards to protect against harmful content.

Google says it will block ad targeting based on factors like age, gender or interests for users under 18. On the other hand, Instagram plans to remove young people's interests but advertisers will still be able to target based on age, gender and location.[17]

Data minimisation and retention

Whatever the child's choice, only the minimum amount of personal data should be collected and retained. Only the elements of your service in which a child is actively and knowingly engaged should collect data.

Child protection

The Code will not prevent deployment of technologies to protect children from online harms such as sexual exploitation and abuse. The EU has recently included an exemption in the ePrivacy Directive to allow accessing or writing data to the user's device without consent when necessary to combat online child sexual abuse.[18] In the UK, there is no such exemption.

Instagram intends to monitor "potentially suspicious behaviour" of users recently blocked or reported by young users and block their ability to see or leave comments on children's posts.

Conclusion

The Code and implementation practice is more mature than it was a year ago. Ongoing regulatory investigations may soon offer further guidance. Organisations are left with little excuse not to comply.

Although the risk-based approach provides flexibility to accommodate commercial goals in some circumstances, others may be inconsistent with the child's best interest and may have to be redesigned.

With other countries showing interest in similar regulation, global action may be in order.

Maya de Silva is Trainee Solicitor and Alexander Dittel is Partner at Wedlake Bell LLP.

---

[1] Age appropriate design code: frequently asked questions for the news media, 2020 (**link**).

[2] Privacy Policy Stadia, 12 August 2021 (**link**).

[3] Age appropriate design code: frequently asked questions for the news media, 2020 (**link**).

[4] Spotify Kids Privacy Policy, 1 September 2021 (**link**).

[5] YouTube Kids Privacy Notice (**link**).

[6] PlayStation Now Privacy Policy, October 2020 (**link**).

[7] DPC, 19 October 2020 (**link**).

[8] DPC, 14 September 2021 (**link**).

[9] Asking People for Their Birthday on Instagram, August 30, 2021(**link**).

[10] Age appropriate design code: frequently asked questions for the news media, 2020 (**link**).

[11] TikTok fined for violating children's privacy, Autoriteit Persoonsgegevens, 22 July 2021 (**link**).

[12] Furthering our safety and privacy commitments for teens on TikTok, August 12 2021 (**link**).

[13] Google to introduce increased protections for minors on its platform, including Search, YouTube and more, 10 August 2021 (**link**).

[14] Nvidia Kids Privacy Policy, May 21 2018 (**link**).

[15] Google to introduce increased protections for minors on its platform, including Search, YouTube and more, 10 August 2021 (**link**).

[16] Google to introduce increased protections for minors on its platform, including Search, YouTube and more, 10 August 2021 (**link**).

[17] Giving Young People a Safer, More Private Experience, 27 July 2021 (**link**).

[18] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance) (**link**).