wiggin

The Children's Code – A quick, practical overview for games businesses

All online businesses that are likely to be accessed by children under 18 must comply with the UK's new Age Appropriate Design Code, also known as "the Code".

The Code has potential to introduce significant new technical, commercial and legal challenges for developers and publishers offering games to players in the UK, regardless of where those developers and publishers are based.

In this video, I'm going to take you through some of the Code's key features and suggest some steps you can take towards compliance.

The Code is a new piece of guidance from the UK's data protection authority, the ICO. The Code doesn't contain 'new law', but instead sets out the standards against which the ICO will measure compliance with existing laws, like the GDPR. While the Code is founded around data protection principles, its overall goal is to protect the best interests of children, and sometimes those interests aren't strictly data related.

The Code applies to "*providers of information society services*", which will include things like online games, apps and YouTube channels, which are "*likely to be accessed by children*". Importantly, children in this context means anyone under 18.

The ICO considers a service as "*likely to be accessed by children*" if it's more probable than not that children may access the service. It's *not* just child-focused games that are caught. The ICO is intentionally casting a wide net and businesses should assume they are caught by the Code unless there's compelling evidence to the contrary.

The ICO has already started enforcing the code and begun reaching out to games businesses to audit compliance. While the ICO is likely to take a pragmatic approach to enforcement, there are early indications the games industry will be a particular focus area alongside social media platforms. Failure to comply with the Code can result in fines of up to 4% of global group turnover or 17.5 million pounds. You could also be prevented from processing children's data.

So what do you actually have to do?

Ultimately, businesses need to make sure that their games are appropriate for the age groups that will play them. So, for example, if your game is predominantly played by players aged 16 or over, you don't need to make everything appropriate for 10 year olds.

Looking at things more practically:

Step 1 is to review each game to determine if it contains any risks to children. The Code highlights several features that are likely to create these risks. Chat functionality is likely to be considered particularly high-risk given the risky user to user behaviours it can facilitate.

Step 2 is to assess whether you can remove or appropriately limit these risks. For example, can you remove the adult content, turn off behavioural advertising for younger users or add automated chat-filters and player reporting functionality.

If you can't remove or limit risks to be age appropriate, Step 3 is to either restrict children from accessing your game at all, or limit children's access to an age-appropriate environment. Alternatively, businesses could opt for a "one-size-fits-all" approach and treat *all* of its users as children, but this could lead to over-restriction.

It may be tempting to attempt to block users under a certain age by using a self-declaration age gate, but whether or not this is acceptable will depend on the risks presented by your specific game. The greater the risks children face if they play your game, the more robust the age verification method must be.

The ICO has indicated that various methods may be appropriate in different circumstances, including self-declaration, AI and the use of third party age verification services. We're expecting more guidance from the ICO on this point soon.

Finally, remember you also need to comply with more general existing data protection requirements. These include minimising data collection, understanding what data is being collected and how it is being used, having clear and age-appropriate privacy documentation and setting privacy settings to high by default. You should also complete a Data Protection Impact Assessment for each of your games, which means keeping a written record of the steps taken to identify and mitigate the risks presented by a particular game.

I hope that's been a useful tour of the new Code. Thanks for watching.