wiggin

THE CHILDREN'S CODE: AN OVERVIEW FOR DIGITAL ENTERTAINMENT BUSINESSES

SUMMARY

1. The Children's Code (also known as the Age Appropriate Design Code) is a new UK statutory code of practice designed to protect children online. It will impact any business offering services to UK users that is "*likely to be accessed by children*". The code expands on the principles set out in the GDPR (e.g. privacy by default).

2. The code will take full effect after a 12-month transition period on 2 September 2021. The UK's data protection authority, the Information Commissioner's Office (**ICO**) will monitor compliance with the code.

3. The code is a new and evolving area of UK regulation. Some businesses may already be on their way towards compliance depending on existing GDPR strategies, though specific preparation is likely to be required. Online services which fall under the scope of the code should revisit their existing data protection strategies and make reasonable and proportional improvements where possible to protect children's privacy. This note contains some general guidance and tips for digital entertainment businesses.

OVERVIEW

What is the Children's Code? The Children's Code is an enhanced toolkit which the ICO will use to assess compliance with existing data protection legislation – so it is not 'new law'. The Children's Code is a set of standards issued by the ICO under the Data Protection Act (DPA) 2018 (i.e. UK's legislative implementation of the General Data Protection Regulation (**GDPR**). It requires that the best interests of children be the "*primary consideration*" when designing and developing online services. The ICO will take compliance with the code into account when considering whether a business has complied with its data protection obligations under the GDPR and/or the Privacy and Electronic Communications Regulations 2003 (**PECR**).

Who does the Children's Code apply to? The code applies to "*providers of information society services*" (including providers of online services such as games, distribution platforms, YouTube channels, apps etc.), which are "*likely to be accessed by children*" (even if children do not actually use the service). The ICO's view is that a service is "*likely to be accessed by children*" if it is more probable than not that "*children*" may access the service, considering factors such as the nature and content of the service, whether it has a particular appeal to children, and any measures in place to prevent children from playing it. "*Children*" is defined as anyone under 18. Other UK regulators (e.g. the Advertising Standards Authority) have previously interpreted similar concepts (i.e. what "*appeals to children*") broadly, so it would not be surprising if the ICO takes a similar approach. This means the code will apply to many online gaming services.

Does the Children's Code apply to businesses based outside of the UK? Yes. The code aligns with the DPA, which means it applies to any services offered to players in the UK, regardless of where the development studio or publisher is based.

What does the Children's Code set out? The code consists of a set of 15 "*flexible*" standards which reflect existing GDPR principles, including:

1. **High privacy settings.** Privacy settings should be high by default unless there is a "*compelling reason*" otherwise. Businesses should not use nudge techniques to encourage children to weaken these settings or share unnecessary personal data.

2. **Geolocation**. Geolocation data is an area of particular concern to the ICO as the data could be used to compromise the physical safety of children. Geolocation options should be switched "*off*" by default unless there is a "*compelling reason*" otherwise. It should be made obvious to the child that their location is being tracked and settings should be reverted to "*off*" after each session (although from the current guidance published by the ICO it is not clear if this means when the app is turned off or minimised).

3. **Profiling**. Profiling is making inferences based on automatically processed personal data e.g. serving personalised advertising content. If profiling is essential to the provision of the core service that the child has requested, it is permitted to be "*on"* by default. Appropriate measures should be in place to protect the child from any harmful effects (e.g. delivering content which is detrimental to their wellbeing or health). Separate privacy settings should be used for each different type of profiling.

4. **Transparency**. Clear privacy information should be provided in language which is suitable for the age of the child. This could be difficult to comply with, given that the ICO's definition of a "*child*" includes individuals up to 18. The ICO recommends providing "*bite-sized"* information about how data is used at the point at which privacy settings are changed (e.g. when location-tracking is on there should be an easy-to-understand pop-up on what will be tracked, for how long, why, etc).

5. **Age appropriate application.** A business should calculate the age range of its audience, then tailor the safeguards it applies based on this range. If a business does not know its audience age, then it should apply safeguards designed for children to its entire userbase since it cannot know which users are children and which are not.

When do businesses have to comply with the Children's Code by? The code came into force on 2 September 2020 but with a 12-month transition period to give businesses time to make any necessary changes. The code will therefore takes full effect on 2 September 2021. The ICO will then consider the code when enforcing the DPA and PECR in matters concerning children's data. The ICO has begun to release additional guidance to help businesses start preparing for the code to come into full effect. For example, the ICO has already launched a Children's Code Hub to help businesses achieve compliance.

What are the penalties for breaching the Children's Code? The code was created under the DPA, breaches of which can result in fines of the greater of £17,500,000 or 4% of annual global group turnover. The ICO has issued a handful of significant fines to-date (e.g. British Airway's £183 million fine and Marriott Hotel's £99 million fine in July 2019 – though both have been appealed and are likely to be reduced significantly if finalised). The majority of these fines have not related specifically to children's data (with the exception of Bounty UK, which was fined £400,000 for illegally sharing the personal information of new mothers and infants).

Breaches of the DPA and/or PECR can also lead to the ICO imposing temporary or permanent restrictions on the use of children's personal data.

HOW COULD THE CODE APPLY TO DIGITAL ENTERTAINMENT BUSINESSES?

Many digital entertainment businesses offer their services to children. Here are some practical examples of how the code will have particular application to digital entertainment businesses:

- The code requires businesses to consider issues that are not directly related to privacy such as screen breaks and general user welfare (e.g. nudge techniques). This could impact business models (particularly for mobile) which reward users for further gameplay/engagement (e.g. reward loops, continuous scrolling notifications and auto-play features).

- Mobile games businesses may face additional challenges given the substantial amount of data collected, particularly for geolocation games which require tracking to play. The ICO warns against using self-declaration age gating (i.e. where a user declares their age without providing any proof) if businesses process high-risk data such as geolocation data.
- Games may be required to segment their audiences and/or tailor experiences appropriately for different age ranges, meaning that certain services would be inaccessible for children. Alternatively, a "*one-size-fits-all*" approach could be taken where all users are treated as children – but this could be overly restrictive.
- Age verification techniques which restrict games to over-18s are likely to become used increasingly to evidence that the code does not impact a game.
- Data sharing between developers and publishers (and other third parties) will become an increasing focus.

The ICO has published a framework which helps companies consider what potential harms their services may include and what may be deemed to be a "*risky activity*" under the code.

5 TIPS FOR COMPLIANCE:

1. **Assess if the Children's Code applies to your business.** This can be done through a Data Protection Impact Assessment (**DPIA**) to identify and minimise any data protection risks. This will in turn help to determine whether the service is likely to be accessed by children. If you have carried out a DPIA before (e.g. for GDPR purposes), then the DPIA templates will need to be reviewed and updated to reflect the code. The ICO has issued a template DPIA here.

2. **Review and/or introduce new age-appropriate resources for your service.** If your DPIA indicates that "*children*" are accessing your services, make sure your privacy documentation is drafted appropriately (e.g. simple language, simple tools, parental controls etc).

3. **Give children high privacy by default.** Consider whether data collected from/about children is needed in the first place. If so, children or their parents should be given choices over any data processing which cannot be justified by a "*compelling reason*".

4. **Review existing age verification mechanisms and introduce new ones where necessary.** The ICO does not mandate a particular age verification mechanism. It does suggest that options such as the use of AI to estimate a user's age or third-party age verification services could be helpful.

5. **Be ready to prove compliance.** The code reemphasises the GDPR's principle of 'accountability' which requires covered businesses to demonstrate (with evidence) that they comply on a technical and organisational level with the code. The ICO has stated it intends to actively carry out audits and affected businesses would benefit from having an audit trail (e.g. DPIAs, intelligible data protection policies, internal training on handling children's data).