TECHNOLOGY AND INNOVATION

Fun-damentals and Games: The DPC's Fundamentals for Processing of Children's Data

January 2021

In this briefing we consider the recent draft guidance from The Data Protection Commission (the "**DPC**") of Ireland on the obligations and best practices in relation to processing children's personal data; the "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing" (the "**Fundamentals**"). The Fundamentals are open for public consultation until 31 March 2021.

1. The Fundamentals consist of 14 fundamentals that were drafted following a detailed public consultation in which the DPC engaged with a range of stakeholders including children. The Fundamentals provide welcome guidance for organisations involved in the processing of children's data and an insight as to what can be expected from future sectoral codes of conduct in this area. The Fundamentals note that the standards the DPC sets for the global internet service providers established in Ireland will affect all child data subjects across the EEA.

2. **Who do the Fundamentals apply to and what approach should organisations take?**

The Fundamentals apply to organisations whose services are directed at, intended for or likely to be accessed by children. In respect of services with both children and adult users the Fundamentals state that ***"likely to be accessed by a child"*** should be understood to mean more likely than not. In an online context this includes websites and apps that provide social media, media sharing, gaming, entertainment, educational, advocacy, health and support services. The Fundamentals also apply to offline services such as educational providers and sports clubs.

Organisations should take steps to identify their users and assess whether the service offered is likely to be accessed by children. Factors such as the nature of the service, its visual content and the presence of celebrities who appeal to children should be considered.

Where a service is accessed by children, an organisation can choose to provide a "floor of protection" so that all users are provided with the same high level of data protection, irrespective of the age of the user. Alternatively, an organisation may take a risk-based approach to verifying the age of users so that the Fundamentals are applied to the processing of personal data of all child users.

3. **Transparency**

Under Article 12 of the GDPR, information about the exercise of the rights of a data subject should be communicated in a concise, transparent, intelligible and easily accessible way, using clear and plain language that is comprehensible to a child. The Fundamentals provide that organisations should consider using formats that are applicable to the service they offer, such as cartoons and videos or layered information.

The Fundamentals emphasise that transparent information should be provided throughout the user experience. In particular, children should receive just-in-time notifications about any potential risks associated with sharing personal data. The DPC advocates an approach whereby children are given the opportunity to ask organisations questions directly regarding the processing of their data. For example, through an instant chat, dedicated email address or privacy dashboard.

The DPC notes that organisations with a mixed audience are not required to provide separate sets of transparency information for adults and children. If information is clear and simple enough for a child to understand, then it will also comply with the requirement of transparency in relation to adult data subjects. Despite this, the DPC emphasise that where the Fundamentals apply, organisations must assess how to ensure meaningful transparency for children, according to the age ranges of child users.

4. **Exercising children's data protection rights**

The DPC does not set a general age threshold for children to exercise their rights but instead considers that a child may exercise their data protection rights as long as they have the capacity to do so and this is in their best interests.

Such an assessment should depend on a number of factors including the nature of the service provided, the personal data being processed and the maturity of the child. Where an organisation decides not to facilitate a child in exercising their data subject rights on the basis that this would not be in the best interests of the child, the organisation should explain the reasoning for that conclusion and inform the child that a request may be made on their behalf.

Where an adult seeks to exercise the data protection rights of a child on the child's behalf, organisations should assess whether it is in the best interest of the child to facilitate such a request. There is a rebuttable presumption under Irish law that a parent / guardian is acting in the best interests of the child unless there is evidence to the contrary. The Fundamentals state that other factors such as the child's age and the nature of the data should also be considered.

5. **Age of consent / age verification**

In Ireland, in order to rely on consent as the lawful basis for processing of children's data, parental consent must be obtained where a child is under 16 years old. The GDPR requires that organisations must make "reasonable efforts" to verify this consent "taking into consideration available technology".

The DPC note that the age of digital consent requirements should not impose restrictions on a child being able to access a service and should not be used as an excuse to 'lock out' children. Similarly, an organisation may not use the digital age of consent or a minimum user age requirement to treat child users as if they were adults. Where an organisation stipulates that a minimum age is required to access their services they should take steps to ensure that age verification mechanisms are effective at preventing children below that age from accessing their service. Otherwise, the organisation will still be required to ensure the appropriate standards of data protection measures are in place to safeguard the position of all child users, regardless of age.

The DPC recognises that there is "no one-size-fits-all solution" to the issue of age verification as the appropriateness of mechanisms will depend on certain factors including the services being offered and the sensitivity of the data being processed. The "floor of protection" method whereby high levels of data protection are applied to processing of data of both adults and children is an alternative approach.

The Fundamentals state there will be a "higher burden" on technology and internet companies in their efforts to verify age and, where required, that consent has been given by a parent / guardian.

6. **Profiling and advertising**

Due to the susceptibility of children to behavioural advertising, one of the fundamentals is a prohibition on profiling children, carrying out automated decision-making concerning children or otherwise using their personal data for marketing / advertising purposes, unless the organisation can clearly demonstrate how and why it is in the best interests of the child to do so.

There is a high burden of proof to demonstrate this with the DPC noting there will be a limited range of circumstances where it can be shown that profiling and / or automated decision making in relation to children are legitimate, lawful activities.

Where children and adults both use a service, the service provider must have means of identifying and protecting children on their platform or else must implement a no-profiling policy across the board.

7. Tools to ensure a high level of data protection

Organisations that the Fundamentals apply to should carry out a data protection impact assessment ("DPIA") in respect of the different types of processing activities which are carried out on data of children. The best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of the organisation in the event of a conflict. Where an organisation decides to profile or engage in automated decision-making about children, a DPIA must be conducted.

A DPIA will assist an organisation with identifying the specific risks to children which arise from processing and to identify the appropriate tools to minimise those risks. What tools are appropriate will vary but the DPC note that measures such as default privacy settings offering the highest level of protection, encouraging privacy-preserving behaviours through the use of push notifications and ensuring user-specific privacy settings can ensure that data protection by design and default is incorporated to "bake in" the best interests of child users.

8. **Next steps**

The DPC has stated that it is preparing to engage with its obligations under the Data Protection Act 2018 to encourage the drawing up of codes of conduct in this area for various sectors. While codes of conduct are not legally binding unless adopted through an implementing act, they are useful guides to assist organisations with satisfying their legal requirements. Codes of conduct can also be used to demonstrate compliance with the GDPR and can act as a mitigating factor when administrative fines are being determined.

The Fundamentals are open to consultation until 31 March 2021. The adoption date and content of the final version of the Fundamentals are likely to depend on the volume and content of responses received by the DPC to its consultation.

The DPC has stated that the final version of the Fundamentals will inform its approach to supervision, regulation and enforcement in the area of processing children's personal data. At this stage, organisations should review any processing of children's personal data and begin to take steps so as to ensure compliance with the Fundamentals that are adopted.

The authors wish to thank Shannon Buckley Barnes for her contribution to this briefing.

KEY CONTACTS

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Aoife Coll
Associate
+353 1 920 1726
aoife.coll@arthurcox.com