GDPR'S CHILDREN DATA REGIME

The best interest of the child v commercial interests

Alexander Dittel Wedlake Bell LLP

If you are operating an online or offline service in Europe or the U.K. that will likely be accessed by children, you are required to comply with a separate regime for the processing of children's personal data. Personal data is not limited to personally identifiable information but includes any obscure online identifier, which means the regime is far-reaching.

The General Data Protection Regulation (GDPR) anticipates specific protection for children because they may be less aware of the risks and consequences of the processing of their personal data, and they may not know their data protection rights. Unless a child has reached the age of digital consent, which is 16 in Ireland and 13 in the U.K, parental consent is required for the processing of children's personal data.

However, the parental consent requirement is only one small aspect of what is required. A person remains a child until they reach the age of 18, and even if they can provide GDPR-compliant consent before then, that does not mean their personal data can be treated like that of an adult. While the GDPR does not tell us much more about the children data regime, the recent regulatory guidance which draws on international law paints a rather complex picture.

The U.K.'s Information Commissioner's Office (ICO) issued its Age Appropriate Design Code (Code). The Irish Office of the Data Protection Commissioner (DPC) issued its Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing (Fundamentals). The Code became effective in September 2021 and the Fundamentals in December 2021. While the ICO is an influential regulator representing a mature online economy, the DPC will act as lead authority for all data processing in Europe carried out by the many U.S. 'big technology' companies that have their main establishment in Ireland.

MAIN OBJECTIVES

Children's personal data must be processed fairly, respecting children's best interests. The Fundamentals go even further by saying that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data. The best interest principle is not only a substantive right but also a fundamental legal interpretative principle under international law.

Children must be supported in exercising their basic rights. The United Nations Convention on the Rights of the Child 1989 (UNCRC) guarantees children the right to access information, the right to develop their own opinion, freedom of expression, the right to play and engage in recreational activities appropriate to their age and much more.

Children must be protected from harms such as online grooming, social anxiety, self-esteem issues, access to harmful or inappropriate content, loss of privacy due to constant monitoring and other harms. Any processing of personal data that gives rise to a risk of such harms will likely not be compliant with the GDPR.

WHAT ARE THE LIMITS OF THE REGIME?

The rules are far-reaching, but they are limited to the processing of personal data. There is a separate legislative effort to address online harms. The U.K. Online Harms Bill aims to improve U.K. citizens' online safety by moderating content, monitoring and taking down illegal and harmful

content. The equivalent EU law, the Digital Services Act, has similar aims.

Unlike these laws, the Code and Fundamentals are not intended to moderate content. Nevertheless, they may indirectly impact content, for example, where personal data is processed to suggest content to young audiences.

The Code promotes a risk-based approach. 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. The ICO expressly wishes to avoid perverse outcomes, such as requiring adult services to become child friendly. While the Fundamentals do not seem to offer such leeway, they are expressed to be 'entirely consistent' with the Code.

WHICH SERVICES ARE IN SCOPE?

While the Code focuses on online services such as social media, marketplaces, search engines and connected toys, the Fundamentals also apply to offline environments, such as the products and services of educational providers, sports and social clubs and communities, and health and social support providers.

The rules apply only if the service is likely to be accessed by children under the age of 18. Even if not aimed at children, your services could be in scope.

KEY STEPS

A simplified approach would consist of the following steps:

STEP 1 – Are children likely to access your products and services? Look at your stats and evidence on user behavior, conduct surveys and map your audiences. It will likely not suffice to just say that your services are not intended for children.

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

STEP 3 – What changes are required to your UI (user interface), service features and product development to best support children's needs? Creativity is in order, but any approach will likely be limited to what is technically possible and the availability of relevant third-party services, such as consent management platforms designed to collect reliable parental consent..

KNOW YOUR AUDIENCE

Children have various competing rights, and the need for each child's protection varies depending on the child's age and maturity. The need for choosing between the child's empowerment or restriction will often arise. Organizations must demonstrate how their approach reflects the assessment and analysis of the best interests given the child's age and developmental capacity.

Ideally, an organization can tailor its services to its audiences. However, if it is unable to determine which user is an adult or a child, it may have to implement a floor level of protection suited to its youngest audiences that will apply to everyone equally. This could come at the cost of commercial exploitation of personal data that may be crucial for the commercial viability of the service.

COMMERCIALIZATION OF DATA

The Fundamentals are quite strict in that they support a prohibition of profiling or targeting of children of any age for commercial purposes based on a digital record of their actual or inferred characteristics. Such activity will likely not be in the child's best interest but rather for the organization's benefit. According to the Fundamentals, with the exception of measures to protect children's welfare or where there is an overriding public interest, there will be a very limited range of circumstances where the profiling of children and the use of automated decision-making concerning children will be legitimate and lawful under the GDPR.

In contrast, the Code will not prevent organizations from using behavioral advertising that the ICO recognizes as an important income stream. However, such advertising must comply with regulatory codes (such as those of the U.K.'s Advertising Standards Authority) that protect children. If based on cookies, advertising must be off by default for child users.

Much data processing for commercial purposes is based on legitimate interest. However, according to the Fundamentals, any legitimate interest will fail if it interferes with, conflicts with or negatively impacts, at any level, the best interests of the child. By contrast, there is no such suggestion under the Code.

Furthermore, the challenge is that organizations cannot circumvent their GDPR obligations by mandating a minimum age to access the services. According to the Fundamentals, shutting children out could deprive them of their rights or force them *underground*. Therefore, age assurance or in high-risk cases, full age verification, will be needed to help organizations classify their users and protect child audience segments. However, even in those cases, the Fundamentals mandate that children's service experience must not be downgraded.

PARENTAL CONSENT

When it comes to parental consent, reasonable efforts must be taken for verification. Emerging technologies offer some hope of maintaining a frictionless user journey, and there certainly is demand for more. The Fundamentals refer to the age verification methods endorsed by the Federal Trade Commission, including:

- Signing a consent form.
- Using a payment card.
- Calling a toll-free number.
- Video conference with trained personnel.
- Providing a copy of ID verified against official database.
- Answering a series of knowledge-based challenge questions aimed at parents.
- Facial recognition ID verification.

According to the Fundamentals, personal data collected for verification must only be used for this purpose and must be deleted afterward.

CONCLUSION

Pursuing your commercial interests is not prohibited, but the best interest of the child must be the primary consideration. Some traditional data monetization activities such as profiling are explicitly discouraged by the Fundamentals and will have to be recalibrated.

Compliance with the legal regime will necessarily involve specialist advice, assessments and some creativity, but according to the Fundamentals, this is the price of doing business with children.

Start with a DPIA, involve all relevant teams, and put your heads together. You may be surprised at how much relevant knowledge there is among your staff who are parents. A child-oriented DPIA should also include a Child Rights Impact Assessment.

Alexander Dittel is partner in the technology practice at Wedlake Bell LLP in London. With more than 10 years of experience in data protection, Alex supports clients with specialist advice on matters involving data in technology, transactions and disputes, as well as general data protection compliance and cyber security matters.