Matheson

"Fundamentals" Protecting Children's Data

New Guidance Published from the Irish Data Protection Commission

On 17 December 2021, the Irish Data Protection Commission ("**DPC**") published its final report (the "**Fundamentals**")[1] detailing its guidance on processing children's personal data, entitled "*Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*".

> "*The Fundamentals have immediate application and operational effect, now forming the basis for the DPC's approach to supervision, regulation and enforcement in the area of processing of children's personal data.*"
>
> (DPC press release, 17 December 2021)

In addition to giving 14 principles for processing children's data, the Fundamentals contains the DPC's advice on:

- particular obligations under the General Data Protection Regulation ("**GDPR**") including legal basis requirements under Article 6, digital age of consent verification under Article 8 and transparency under Article 12; and
- the ability of children to assert their own data protection rights and the ability of parents and guardians to assert data protection rights on their child's behalf.

This article will outline the scope of these Fundamentals, the Fundamentals themselves, guidance on GDPR obligations and outline how a child's data protection rights can be exercised.

Contents

[1] DPC, Fundamentals for a Child-Orientated Approach to Data Processing (December 2021)

PART 1: SCOPE OF THE FUNDAMENTALS

The Fundamentals are addressed to organisations whose services are "*directed at, intended for or likely to be accessed by children*." The "*core message ...is that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data*."

Applying to both online and offline organisations, this cuts across a broad spectrum of industries from educational providers, sports and social clubs, health and social support providers through to websites, apps and other Internet of Things ("**IoT**") services. The DPC makes clear that the Fundamentals are to cover services that a significant number of children are in reality using (as opposed to any service that is offered online).

The DPC has taken into account a broad spectrum of voices, including those of children, as well as the "Age Appropriate Design Code" for online services processing children's data of the UK Information Commissioner's Office ("ICO"). The DPC noted that its focus was broader than the ICO's as DPC was not focused solely on the engineering and design of online products and services. The Fundamentals are viewed by the DPC as consistent with the UK Code. In addition, the DPC has reinforced its commitment to child data protection by reference to the Court of Justice of the European Union and the European Court of Human Rights recognising the binding nature of the UN Convention on the Rights of the Child.

Questions are raised and, where appropriate, answers given by the DPC around digital age of consent, capacity, online harms, advertising that rely on tracking and profiling, "mixed use" internet environments, online and offline contexts and more.

Read More: Matheson Bulletin - Ready to Enter the Metaverse?

"Even if the GDPR hadn't told us so, it is very clear that children warrant special protection when it comes to the processing of their personal data. After all, in every other area of society, be it sport, education, access to alcohol, or voting rights, the special position and the evolving capacities of children are universally recognised facts. We have an opportunity now to correct issues of unwarranted and high-risk processing of children's data that may have been unwittingly or even negligently implemented across many sectors. The DPC is determined, through these "Fundamentals", to drive that transformation in how the personal data of children is handled."

Helen Dixon, Data Protection Commissioner

PART 2: THE FUNDAMENTALS

The 14 Fundamentals are summarised as follows:

01 **FLOOR OF PROTECTION:** Unless using a risk-based approach to verify users' ages, organisations should provide a default "*floor*" of higher protection for all users irrespective of whether they are a child or not. If organisations choose not to apply the "*floor*", then they are to take a risk-based approach. Organisations may want to consider their options more broadly in light of the EU Single Digital Market legislation, EU Artificial Intelligence Regulation and Irish legislation soon to be enacted Consumer Rights Bill 2021.

02 **CLEAR-CUT CONSENT:** Organisations should obtain "*clear-cut consent*" from a child if relying on consent as a basis for processing.

03 **ZERO TOLERANCE:** When an organisation is relying on legitimate interests, this must not conflict with or override a child's best interests. The Fundamentals says **there should be "zero interference" with the best interests of a child**. In the earlier consultation report, the DPC said it had received "*significant pushback*" on the zero interference concept. The DPC's response is that while controllers are not prohibited from relying on legitimate interests to process child data, no level of interference of child data subject interests should be allowed for. This is because of the GDPR's explicit mention of the need to protect child data subjects when legitimate interests are relied on. The DPC did clarify that in situations where the interference with the child's best interests could be mitigated such that there is "*no resultant interference*", this would comply with the zero interference principle.

04 **KNOW YOUR AUDIENCE:** Steps should be taken to identify a service's likely audience and whether this includes children. In the consultation report, concerns were expressed that this would require collecting additional information about users in contravention of data minimisation. The DPC did not accept this point.

05 **INFORMATION IN EVERY INSTANCE:** Children must be notified of the basis on which their data is being processed, regardless of what that basis is (including parental consent under Article 8).

06 **CHILD-ORIENTED TRANSPARENCY:** Required information must be provided in a language suitable to the age of the child throughout their experience, using non-textual measures if appropriate.

07 **LET CHILDREN HAVE THEIR SAY:** Children are equivalent to adult data subjects in terms of exercising their rights, and may do so at any time once they have capacity and it is in their best interests to do so (discussed further below).

08 **CONSENT DOESN'T CHANGE CHILDHOOD:** Organisations must not treat a child's personal data the same as that of an adult simply because the child's consent or consent from their parent or guardian has been obtained. Children's data must be afforded "*specific protection*".

09 **YOUR PLATFORM, YOUR RESPONSIBILITY:** Companies that derive revenue from providing or selling services online are expected to "*go the extra mile*" in ensuring their age and parental consent verification methods are effective. A significant portion of the earlier consultation report deals with responses to age verification aspects of the Fundamentals. Respondents queried whether GDPR actually requires this and claimed that no risk-free age verification system exists. The DPC says that the GDPR requires special treatment of child subjects, and if controllers elect not to differentiate them (because they fail to use adequate or any age verification methods), a "*floor*" of protection should be provided for all users as if they were child subjects (see Fundamental No. 1, above).

10 **DON'T SHUT OUT CHILD USERS OR DOWNGRADE THEIR EXPERIENCE:** Organisations should not "*shut out*" or create a two-tiered service experience between children and adults on the basis of purported compliance with data protection obligations.

11 **MINIMUM USER AGES AREN'T AN EXCUSE:** GDPR obligations and DPC expectations under the Fundamentals are not displaced by uniform "*theoretical user age thresholds*". Organisations must either put in place adequate age verification methods to ensure nobody under the stipulated age may access the service, or provide data protection measures appropriate to protect children's data (based on the assumption that inadequate age verification measures will be circumvented by children).

12 **A PRECAUTIONARY APPROACH TO PROFILING:** Children's data should not be used for profiling or automated decisions for marketing or advertising purposes unless it can be "*clearly demonstrated*" that doing so is in the child's best interests.[2] Children must be made aware of their right to object to the use of their data for direct marketing purposes. The DPC goes into greater detail around adtech, profiling and direct marketing.

13 **DO A DPIA:** Data Protection Impact Assessments ("**DPIA**") should consider risks particular to children. The child's best interests "*must prevail over... commercial interests*" in the case of a conflict. The DPC has recognised the benefits of conducting a Child Rights Impact Assessments as a tool for translating the best interests of the child principle into practice, and demonstrating compliance with Article 24 (responsibility of the controller) and Article 25 (data protection by design and by default) of GDPR.

14 **BAKE IT IN:** Where children's data is routinely processed, controllers should "*bake in*" a high level of data protection across their services by default. In the prior consultation report, the DPC stated that adhering to GDPR requirements and the child's best interests are "*a crucial and necessary component of running a business that profits or benefits from having children as a central cohorts of its user population*." The DPC has provided recommend measures for incorporating data protection by design and by default to promote the best interests of child users, outlined in the box below.

[2] **The DPC considers that instances where this applies will be limited, potential examples being direct marketing of counselling services, education, health or advocacy organisations.**

PART 3: GUIDANCE ON GDPR OBLIGATIONS

The GDPR's Recitals state that children's personal data should be given "*specific protection*",[3] with children to be borne in mind when organisations are to communicate in "*clear and plain language*".[4] Of most relevance in terms of substantive provisions are Articles 6, 8 and 12 of the GDPR, which deal with legal bases for processing, processing children's data with consent and transparency.

Consent - Article 6

The DPC advises controllers to **consider alternative bases to processing children's data which is necessary for the performance of a contract**, given the complexities around children's competence to enter into contracts in Irish law (Article 6(1)(b) GDPR). Consent must be freely given, specific, informed and unambiguous, with the possibility of it being withdrawn anytime. This will be interesting to see actioned, especially in light of cookies and the broader reduction in use of third-party cookies, particularly those relating to advertising.

The DPC provides city, and notes the limitations as to the minimum age of digital consent – currently 16 years in Ireland (with contract being voidable in Ireland in most instances where person is under 18 years).

Under Article 6(1)(d) GDPR, allowing processing to protect a vital interest, the DPC notes that the threshold for determining a "*vital interest*" is lower in the context of children, and that data protection considerations should always be superseded by child welfare. Also noteworthy is the DPC's statement that data protection laws "*are not a barrier to safeguarding (children), and that it is in the best interests of children to be protected from violence, abuse or interference / control by any party.*"

Article 6(1)(f) GDPR states that processing for legitimate interests can be outweighed by the interests or fundamental rights and freedoms of data subjects, "*in particular where the data subject is a child*". The Fundamentals states that there should be "*zero interference*" with the best interests of a child, and that these best interests should prevail over a controller's commercial interests in the event of any conflict. The Fundamentals also applies this interpretation to instances where organisations might rely on legitimate interests to engage in non-electronic direct marketing, stating that the child's best interests must not be impacted "*at any level*".

Information Society Services - Article 8

Article 8 GDPR applies when providers of information society services[5] process children's data on the basis of consent. Under GDPR as implemented by the Data Protection Act 2018 (the "**2018 Act**"), where such providers are "*offered directly*" to a child, processing of that child's personal data by consent is only lawful if (a) the child is over 16 years old; or (b) the child is less than 16 and consent is received from a person with parental responsibility over the child. Controllers are also obliged under Article 8(2) to "*make reasonable efforts*" to verify that a person with parental responsibility for the child has in fact authorised processing of the child's data.

The DPC agrees with recent guidance from the European Data Protection Board ("**EDPB**")[6] in suggesting a proportionate but not overly intrusive approach should be taken to organisations' obligations under Article 8(2). The Fundamentals give examples such as signing a consent form, using an online payment system which notifies parents of each transaction, video conference or by verifying a parent's photo ID. The DPC also says that when determining which age verification steps are reasonable, the bar will be set higher for technology and internet companies.

The Fundamentals mention that the age of digital consent also likely applies to electronic methods of direct marketing, meaning consent to direct marketing by electronic means may only be given by children over 16 or by a child's parent or guardian. The DPC says that while this technically means that non-electronic methods of direct marketing could be carried out on the basis of consent of children of any age, organisations should be "*extremely cautious about doing so*" and must ensure general GDPR requirements around consent, transparency and respecting the best interests of the child are adhered to.

Transparency - Article 12

The Fundamentals contains a distinct section on transparency under Article 12, 13 and 14 GDPR. As is the case for adult subjects, children are entitled to receive information about the processing of their data in clear and plain language. The points around clear and plain language has been given importance for broader consumers as part of the EU Digital Single Market, for example in digital marketing pursuant to the EU Directives 2019/770 (Digital Content Directive) and 2019/771 (Sale of Goods Directives) which is due to be implemented by the Irish Consumer Rights Bill 2021. If the "*floor*" is to be applied holistically then organisations may wish to consider their obligations with these EU Directives.

Organisations are expected to "*know their audience*" and tailor their communications for "*optimum accessibility and understandability*". In this regard, the DPC says that organisations should consider adjusting the language and vocabulary used in their communications to children or utilising non-textual methods to communicate such as cartoons or videos. The Fundamentals also recommends that organisations make themselves readily available to answer children's questions on processing via an instant chat, email or a "*privacy dashboard*."

[3] Recital 38, GDPR

[4] Recital 58 and Article 12, GDPR

[5] Defined in Directive 2015/1535 at Article 1(1)(b): "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services", and by case law, for example the Uber case (C-434/15) in which it was held that Uber was not an ISS provider as its service was more than solely acting as an intermediary connecting drivers and passengers, which was only one part of its principal service offering which was held to be in the field of transport.

[6] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

PART 4: EXERCISING A CHILD'S DATA PROTECTION RIGHTS

Children Asserting their own Data Protection Rights

The DPC is of the view that a child who understands the nature of their rights and is acting in their best interests is capable of asserting their data protection rights as if they were an adult. Children are not deprived of any data protection rights enjoyed by adults[7], though Irish law does not specify an age at which children may assert their data protection rights themselves.[8]

The Fundamentals state that age alone should not be decisive, and the DPC stands by this position in the prior consultation report. Instead, the DPC says the following factors should also be considered:

- maturity;
- the type of request (e.g. DSAR, erasure, objection to processing);
- context of processing and service provided;
- type of personal data;
- whether enabling the child to exercise their rights is in their best interests; and
- whether the child is assisted by a parent, guardian or third party advocate.

In the prior consultation report, the DPC said that some responses claimed that the DPC was not considering the variation in needs between young children and teenagers, and that the Fundamentals should provide a specific age threshold so as to remove the burden from online service providers. In response, the DPC says that it considered very carefully the setting of specific age thresholds, but due to the varying cognitive development in children it would be inappropriate to do so. The DPC refers to a child's fundamental right to be heard when they are capable of expressing their own views, and says that a hard-age threshold for exercising data protection rights would not respect this right.

Concerns were also expressed about controllers' abilities to assess a child's capacity, with suggestions that this decision should be left to the child's parents or guardians. While the DPC appreciates that additional resourcing will be required for this purpose, they say that this is an obligation inherent in an organisation's decision to process children's personal data and is an "*unavoidable feature*" of doing so.

Added to this the DPC acknowledged that large-scale online platforms and digital service providers will millions of users will likely rely upon automated tools for the purposes of enabling data subject to exercise their data protection rights. For child users, DPC asks organisation to have dedicated, clear and child-friendly user flows in place to facilitate children to exercise their rights. This will be even more important with future tech developments, especially connected to the Metaverse.

Finally, the DPC makes the point that if a controller is comfortable offering services to a child in such a way that the child is autonomously engaging with the service, such child users will likely be in a position to exercise their own data protection rights in relation to that service.

[7] Including situations where the basis of processing is consent by their parent/guardian.

[8] By contrast, DPC pointed in its consultation report that there is a presumption that a child over 12 may do so in Scottish law.

Parental Assertion of a Child's Rights

The DPC says that parents and guardians may access their child's personal data once doing so is in the child's best interests.[9] There is a rebuttable presumption in Ireland that a parent is acting in their child's best interests, in addition to which the DPC says the following factors should be considered:

- age – the closer to 18 the more appropriate it is for the organisation to deal with the child themselves. Parents of a child over 17 should only be capable of exercising that child's rights in "*exceptional circumstances*";
- nature or sensitivity of the personal data;
- nature of the relationship between parent and child;
- purpose for which the parent is exercising the child's rights other than the child's best interests;
- the child's view and whether they consent/would consent to the parental exercise of their rights;
- potential harm or distress to the child of allowing the parent to exercise their rights; and
- whether any sectoral rules apply.[10]

CONCLUSION

The Fundamentals are a result of a detailed and carefully considered consultation by the DPC. It is reported as a clear recognition of the DPC's continued drive to transform how the personal data of children is handled.

No transitional or grace period will be afforded to data controllers following publication of the Fundamentals. Organisations engaging in the processing of children's data must therefore be cognisant of how they are currently treating this data, with the DPC likely to focus enforcement against those who fail to provide the levels of protection envisaged in the Fundamentals. Organisations are expected to know their audience and adjust accordingly. Finally, organisations should be aware of the DPC's recognition of the ability of both a child and their parents to assert the child's data protection rights – with the expectation that decisions taken will always represent the child's best interests.

[9] McK v The Information Commissioner (2006) IESC 2.

[10] For example, parental ability to access child's school records under the Education Act 1998.

PART 5: KEY CONTACTS

Matheson's highly experienced **Technology and Innovation Group** are available to discuss any aspects of these important Fundamentals with you, please do not hesitate to get in touch.

Anne-Marie Bohan
Partner | Head of Technology and Innvation
T +353 1 232 2212
E anne-marie.bohan@matheson.com

Rory O'Keeffe
Partner | Technology and Innovation
T +353 1 232 2000
E rory.o'keeffe@matheson.com

Deirdre Crowley
Partner | Technology and Innovation
T +353 1 232 3710
E deirdre.crowley@matheson.com

Carlo Salizzo
Senior Associate | Technology and Innovation
T +353 1 232 2000
E carlo.salizzo@matheson.com

Davinia Brennan
Partner | Technology and Innovation
T +353 1 232 2700
E davinia.brennan@matheson.com