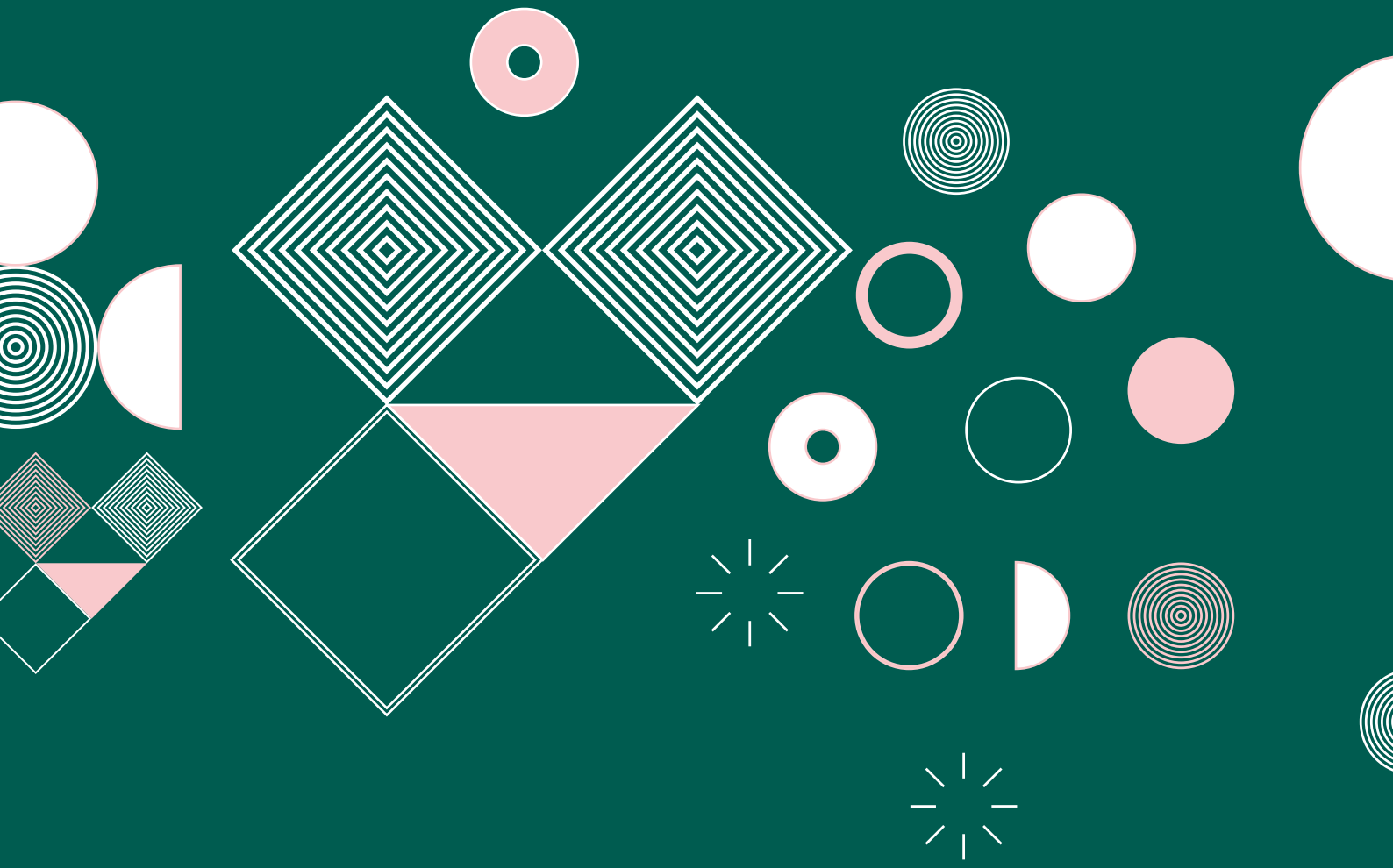
Data Protection Commission

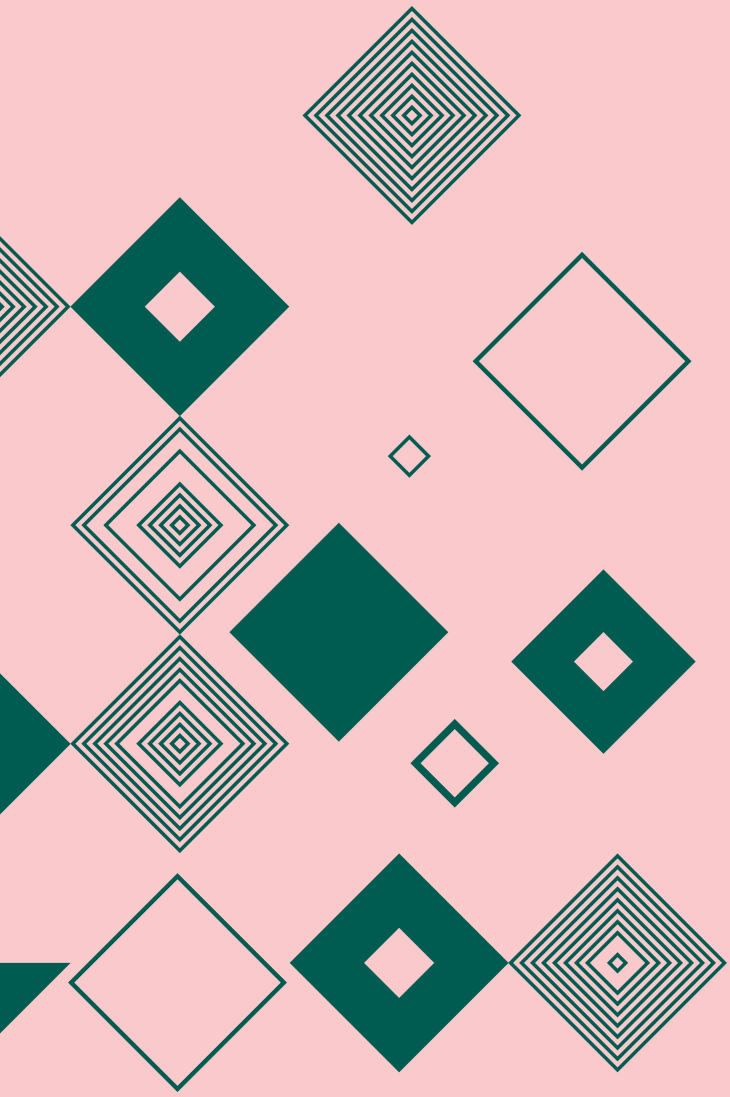
Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing

REPORT ON PUBLIC CONSULTATION

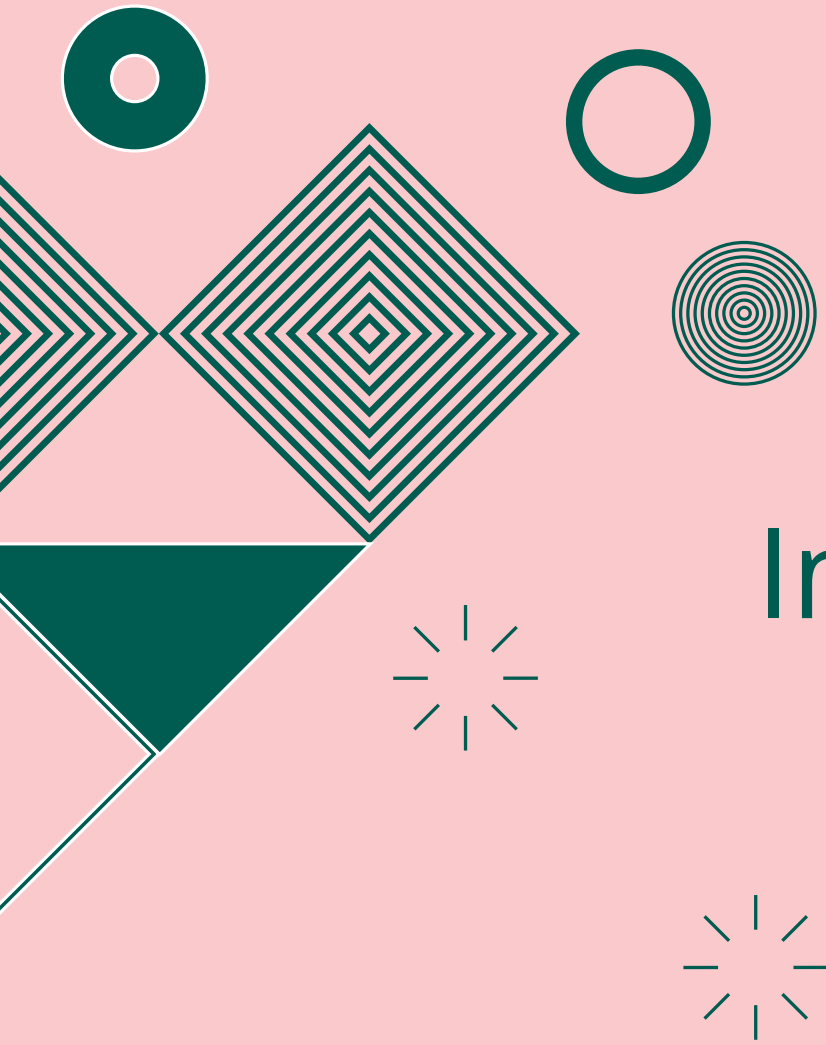


An Coimisiún um Chosaint Sonraí
Data Protection Commission

NOVEMBER 2021
DATA PROTECTION COMMISSION,
21 FITZWILLIAM SQUARE, DUBLIN 2



Contents



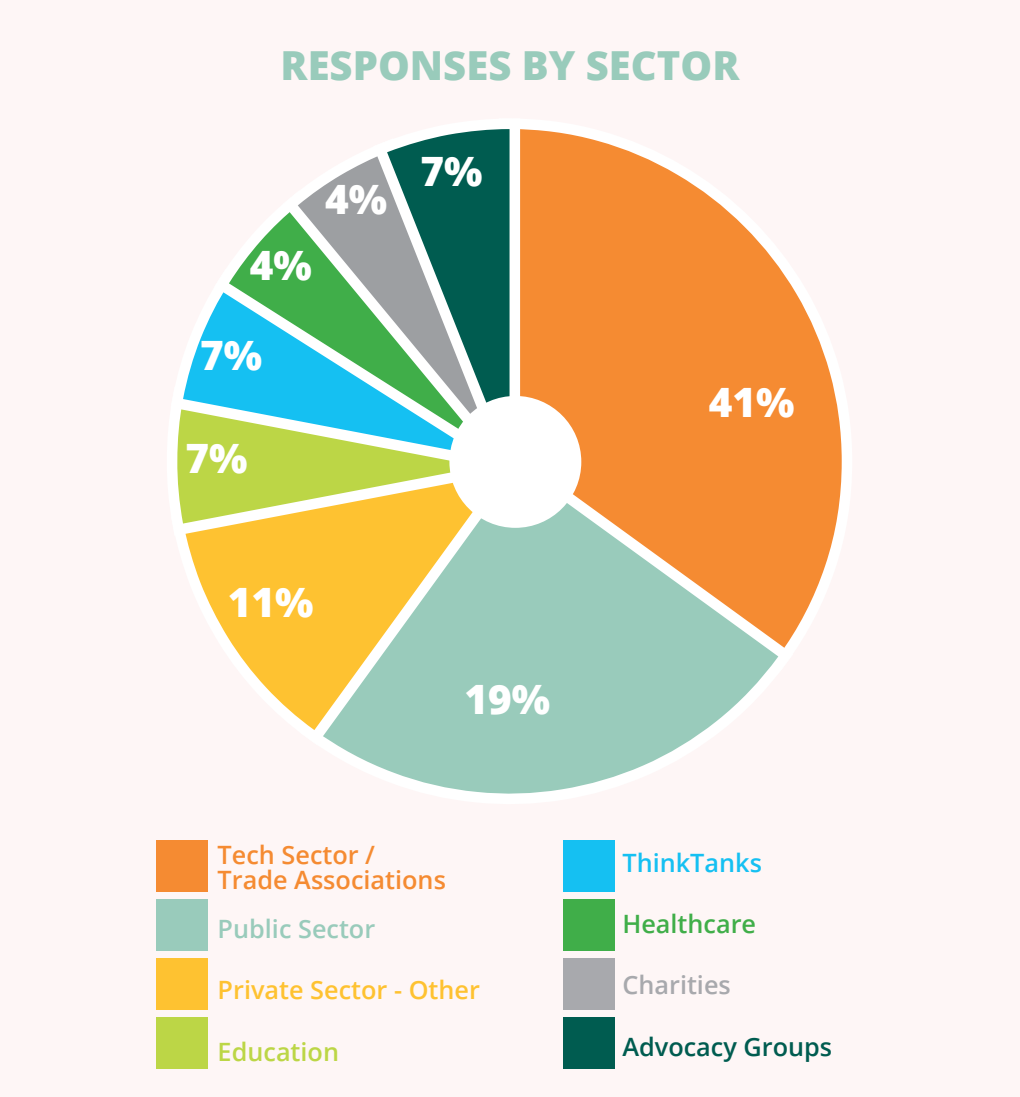
Introduction

INTRODUCTION

In December 2020, the Data Protection Commission ("DPC") published draft guidance entitled "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing" (the "Fundamentals"). The Fundamentals were informed by the output of the two-streamed public consultation which the DPC ran during the first half of 2019, as well as by extensive legal analysis and expert input from key child rights stakeholders over the course of 2019 and 2020.

Between 18 December 2020 and 31 March 2021, the DPC ran a public consultation on the draft version of the Fundamentals to give stakeholders a final opportunity to present their views. This report summarises the key themes emerging from the submissions received. The DPC received 27 written responses to the consultation, and is grateful to those who took the time to comment. A copy of the submissions received from organisations is available on our ***website.*** The DPC has been carefully considering the comments and views expressed in the submissions received and these will inform the DPC's work in finalising the Fundamentals. The DPC has also included in this report its own views on some of the key themes emerging from the submissions to the consultation on the Fundamentals.

CONSULTATION SUBMISSIONS



As demonstrated in the above chart, the majority of submissions received were from the technology sector, both from companies and from trade associations representing a number of organisations from this sector. A variety of issues were raised during the consultation, and some submissions covered more sections of the guidance than others. While it is not possible to cover every point in detail, the DPC has summarised the responses received across those aspects of the Fundamentals that attracted the most feedback from stakeholders, which were as follows:

SECTIONS OF THE GUIDANCE THAT ATTRACTED THE MOST FEEDBACK

In addition, this report also gives an indication of the types of stakeholder views and comments received across each section of the Fundamentals. There are also some overarching themes which the DPC has identified from the submissions which cut across a number of the 14 principles set out in the Fundamentals.

GENERAL COMMENTS ON THEMES EMERGING FROM THE CONSULTATION

The majority of submissions welcomed the DPC's guidance and were supportive of the intention of the Fundamentals, recognising the importance of the protection of children's personal data and of children as data subjects, and the need for guidance on this topic. There was also widespread support for the methodological approach taken by the DPC in producing the Fundamentals, namely the extensive research conducted and consultation process undertaken with children and adults that underpins the guidance. Most submissions also welcomed the DPC's focus on the centrality of the best interests of the child as a guiding principle throughout the Fundamentals.

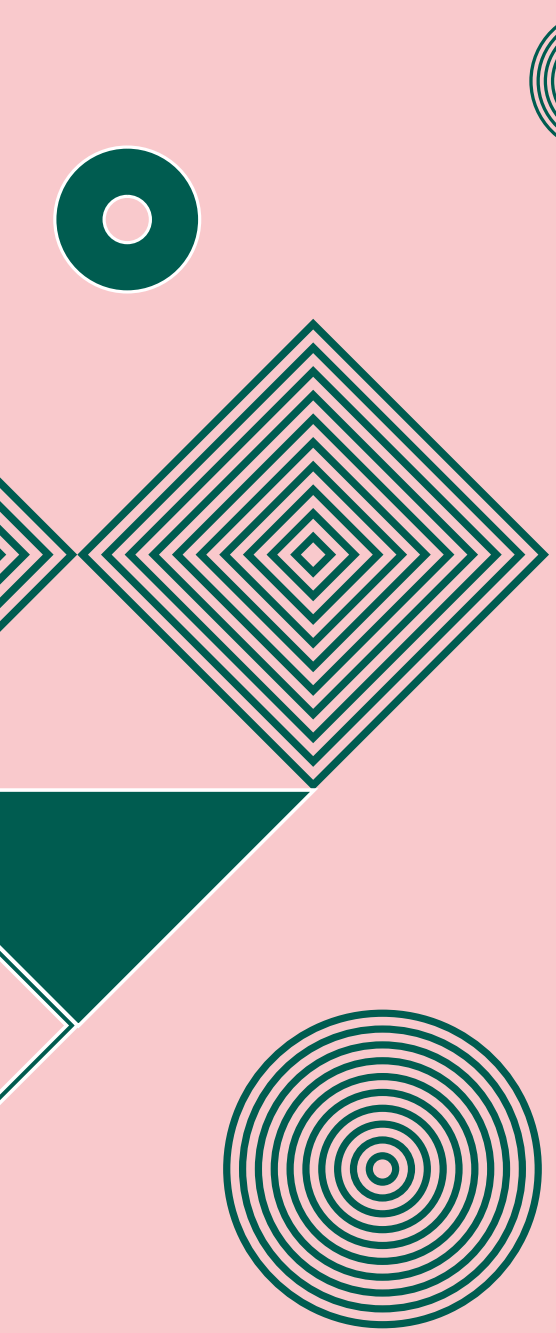
However, it also must be said that the DPC was rather surprised by the general tenor of some submissions, particularly from the technology sector or trade associations representing organisations from this sector. The GDPR sets out high-level obligations which are imposed on controllers who process the personal data of children. In the draft Fundamentals, the DPC sought to clarify – for the benefit of both controllers and children alike – the principles arising from these obligations to which the DPC expects controllers to adhere. While the purposes of the DPC's consultation on the draft Fundamentals was to invite feedback on this draft document, many submissions from industry appeared to want wholesale sections of the document removed without suggesting alternative approaches which would still afford the same high level of protection to child users of services. It is notable in this regard that organisations, which purport to already have effective and proportionate safeguards in place for protecting children's personal data within their service, objected to core aspects of the principles set out in the draft Fundamentals, for example opposing the core foundational principle that the guidance should apply to all children under 18 or to services that are "likely to be accessed by children", and asserting that the DPC's position on profiling and zero interference with a child's fundamental rights and freedoms was excessive and out of step with the views of other regulators.

As the DPC has made clear at every stage of this project, one of the core objectives of the Fundamentals is to clarify the standards that apply to the processing of children's data in both the digital and offline environments. The topics addressed by the Fundamentals were identified and developed by the DPC throughout the course of extensive dialogue with a broad range of stakeholders, including, of course, with children themselves.

The DPC considers it critical that children are recognised as a distinct cohort of users of services, especially in the online world, who are data subjects in their own right and who merit specific protection. Organisations operating platforms and services which are popular with children have a key role to play in driving this cultural change so that SMEs and market entrants with finite resources can follow suit. In the DPC's view, it is vital that organisations accept that the best interests of the child and the specific requirements demanded by the GDPR for the protection of children's personal data are

a crucial and necessary component of running a business that profits or benefits from having children as a central cohort of its user population.

The DPC acknowledges that the entities to whom the Fundamentals are addressed between them process hundreds of millions of child users' personal data, be they global online platforms, local sports clubs or public sector organisations. Preparing guidance which is of general application to every sector, and which frames the intention of the GDPR to provide for specific protections for children, is a challenging objective. Bearing this in mind and consistent with the principle of accountability, the DPC recognises that ultimately controllers have discretion in making decisions to ensure that they give effect to the specific protections the GDPR requires them to implement where children are concerned. However, the existence of this discretion does not imply an excuse for inaction, inertia or rejection of the Fundamentals. The best interests of the child must ground the actions of all data controllers, and there must be a floor of protection below which no user, and in particular no child user, drops.



Scope of the Fundamentals

1. SCOPE OF THE FUNDAMENTALS

1.1 "Likely to be accessed by"

Opinions amongst respondents were divided on the scope of the Fundamentals applying to organisations whose services are "likely to be accessed" by children. Some submissions (particularly from the technology sector) felt that the term "likely to be accessed by" could potentially extend to any service offered online, including incidental, unintentional or limited access to a service by a child, when the service is otherwise not specially tailored to children as part of the organisation's core business. On the other hand, submissions from advocacy groups, public sector bodies and private sector organisations highlighted this criterion as crucial and as one of the key strengths of Fundamentals.

DPC response: The DPC's approach to regulation in this area is not solely concerned with organisations whose services are overtly directed at, or intended for, children. In our experience, it is often those organisations whose services are not exclusively aimed at children but which are nevertheless frequently used by them that present the biggest issues from a data protection perspective for child users. In addition, some submissions asserted that the proposed scope of the Fundamentals will require any service offered online to comply with the Fundamentals. This is not the case and it is important to note that Section 1.3 of the draft Fundamentals clearly states that the phrase "likely to be accessed by a child" refers to situations where this is "more likely than not" to be the case. This scope is intended to cover services that a significant number of children are *in reality* using, even if the service in question was not primarily intended for children or originally designed with them in mind.

The principle of accountability under the GDPR requires organisations to take appropriate steps to determine in the first instance whether they are collecting the personal data of children and thereafter, to ensure that they comply with the higher standards of protection required of controllers under the GDPR with regard to the processing of children's data. Furthermore, General Comment No. 25, of the UN Committee on the Rights of the Child, on children's rights in relation to the digital environment[1] (which was published after the draft Fundamentals were published) highlights that all businesses that impact upon children's rights in relation to the digital environment should be required to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services, and that this includes businesses "*that target children, have children as end users or otherwise affect children*".

For these reasons, the DPC is satisfied that the application of the Fundamentals to organisations whose services are likely to be accessed by children is the right approach. Narrowing the scope of the Fundamentals in the manner suggested by some submissions may create the effect that organisations simply declare that their service is not directed at or intended for children, which in turn would not only undermine, but potentially completely negate the level of protection afforded to children online which is

[1]General Comment No. 25 on children's rights in relation to the digital environment was published on 23 March 2021. Available here: ***https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en***

intended to be achieved by this principle. **Organisations must recognise that they have an obligation to objectively assess by way of an evidence-based approach whether their service falls within the scope of the Fundamentals.**

While the DPC remains of the view, having considered the consultation responses, that the formulation of "likely to be accessed by" would not be reasonably interpreted as meaning "any service which a child could possibly access on the internet", the DPC is nevertheless considering revisions to the relevant text in order to add further clarity to this central building block of the Fundamentals.

1.2 Definition of children as a cohort

The Fundamentals clarify that in Ireland, for data protection purposes, a child is somebody under the age 18[2]. While some submissions highlighted the importance of the Fundamentals' recognition that anyone under 18 is a child, others expressed concern that the DPC had not accounted for the evolving capacities of children and that extending the Fundamentals to all young people under 18 disregarded the abilities and needs of teenagers, and would limit their autonomy, access to information, and digital development.

DPC response: Throughout the consultation and drafting process, the DPC has engaged extensively with experts in the field of children's rights and child protection and has carried out significant legal and literature-based research into children's rights at both an Irish and international level. Article 1 of the UN Convention on the Rights of the Child (the "UNCRC") defines a child as "a person under the age of 18 years"[3], as does the Data Protection Act 2018. The GDPR does not define a child but Article 8 of the GDPR indicates that consent of the child can be relied on by a controller when 'the child is at least 16 years old' (or lower where this is provided for by national law; the relevant age is 16 in Ireland). As the ICO has pointed out, there is therefore "*no implication in the GDPR that children cease to be children when they reach the age at which they can provide consent to the processing of their own personal data*"[4]. Based on the DPC's research, a common theme that appears to be interwoven throughout key academic texts on children's rights is the concept of childhood as a protected space, and that childhood lasts until the individual reaches the age of 18. Prominent child rights advocacy group 5Rights Foundation states that children under the age of 18 are "*entitled to the privileges and protections set out in the UNCRC*"[5].

The DPC acknowledges the importance of respecting the evolving capacities of the child (which is one of the cornerstone principles of the UNCRC), and strongly encourages data controllers to incorporate this into the design and operation of their services, as well as taking this concept into account when it comes to dealing with child data subjects

[2]See Section 29 Data Protection Act 2018
[3]Unless the applicable law specifies otherwise
[4]See the ICO's report on responses to their public consultation on the Age-Appropriate Design Code, available at: ***https://ico.org.uk/media/about-the-ico/consultations/aadc/2616996/summary-of-responses.pdf***
[5]5Rights Foundation. *But How Do They Know It Is A Child? Age Assurance in the Digital World*. March 2021 Available at: ***https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html***

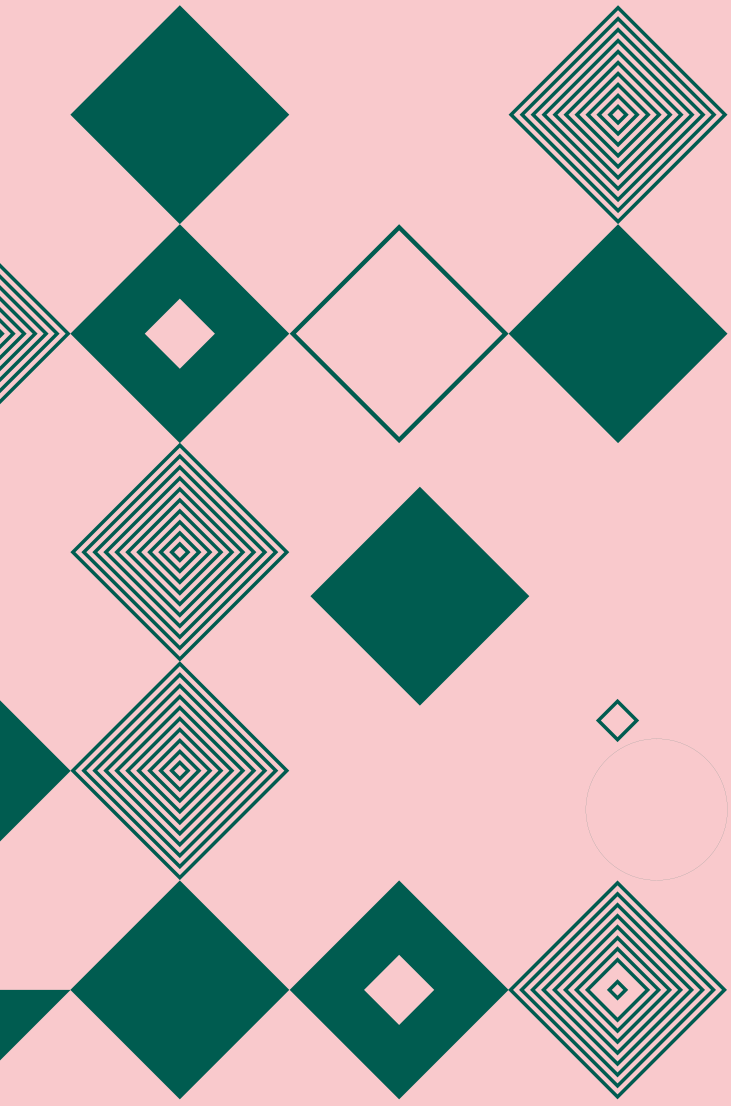
who may wish to exercise their own rights. It is important to point out however that the requirement in Article 5 of the UNCRC that appropriate guidance and direction is provided to children in the exercise of their rights in a manner consistent with their evolving capacities, is not an invitation for children to be treated as adults. Instead, protective measures should be introduced which acknowledge children's capacities as evolving but not yet fully evolved[6]. Further, in order for data controllers to be able to do this, they firstly need to know that they are dealing with a child, and secondly the age range of that child.

1.3 Status of the Fundamentals and implementation period

A number of submissions raised questions about the legal status of the Fundamentals and whether an implementation period will be granted to data controllers upon finalisation of the guidance. Some submissions also questioned how the DPC plans to monitor compliance with the Fundamentals.

DPC response: The Fundamentals is a substantial guidance document consisting of child-specific data protection interpretative principles, and while it does not have statutory underpinning (as, for example, the ICO's Age-Appropriate Design Code does[7]), it will inform the DPC's approach to supervision, regulation and enforcement in the area of processing of children's personal data. In light of the risks posed to children by the processing of their personal data, particularly in an online context, and the pressing need for important cultural changes and significant improvements in child-protective measures, **upon publication in final form, the DPC's intention is that the Fundamentals will have immediate effect and there will be no lead-in period for compliance**. This reflects the fact that the Fundamentals are not a statutory code and there is no requirement to have a lead-in period for any guidance which the DPC produces. Furthermore, the GDPR is now more than 3 years into its application. Organisations which process children's personal data – particularly in the digital sectors where business models are predicated upon the processing of personal data for the provision of services – should throughout that period, in line with their accountability obligations under GDPR, have been constantly keeping their child protective measures under review and revision in order to achieve the higher standards of protection which the GDPR requires in relation to the processing of children's data.

[6]Innocenti Insight: The Evolving Capacities of the Child, Gerison Lansdown (2005)
[7]This was required to be prepared by the ICO under Section 123 of the UK Data Protection Act 2018



Legal backdrop

2. LEGAL BACKDROP

2.1 Best interests of the child

The Fundamentals are anchored on the principle of the best interests of the child, a principle which derives from international law (the UNCRC which forms part of EU and national law). This requires that the obligation to act in the best interest of the child is paramount when considering the position of children as data subjects and in any context where decisions are made by any organisation in connection with the processing of children's personal data. The best interests principle should be a primary consideration in all decisions made when processing children's personal data, and Fundamental Nos. 3 ("Zero interference") , 7 ("Let children have their say"), 12 ("Prohibition on profiling"), and 13 ("Do a DPIA") specifically call out the importance of carrying out this assessment.

While most submissions reflected support for the DPC's focus on the importance of the best interests of the child, some submissions expressed the view that the DPC was not taking an holistic approach to the application of the best interests of the child principle and was placing too much emphasis on the child's right to privacy under the UNCRC instead of weighing that right against all of the other rights that children enjoy under the UNCRC.

DPC Response: The DPC firstly makes the point that the Fundamentals are about the Charter-protected[8] right to the protection of one's personal data. The Fundamentals have been produced for the purposes of clarifying the principles, arising from the high-level obligations under the GDPR, to which the DPC expects organisations which process children's personal data to adhere. Given the DPC's remit as a supervisory authority under the GDPR, the Fundamentals have not been produced for the purposes of giving effect to Article 16 UNCRC (the child's right to ***privacy*** under international law) although many of the issues in the Fundamentals may converge with that right.

However, in preparing the Fundamentals, as explained in the draft document, the DPC has used interpretative principles[9] from the UNCRC given that the UNCRC – as explained in Section 2 of the Fundamentals – forms a central feature of the legal backdrop to children's rights. The DPC fully appreciates that there is no hierarchy of rights under the UNCRC and that an holistic approach to the application of the best interests of the child principle is required when considering the rights of the child. At the same time, the DPC does not accept the framing of the issues as described in some submissions namely

[8]See Article 8 of the Charter of Fundamental Rights of the EU. For the full text of the Charter, please see ***https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT***

[9]See paragraph 1 and 6 of the UN Committee on the Rights of the Child, General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*. Available at: ***https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.*** See also the UN Committee on the Rights of the Child General Comment No. 5 at paragraph 12 which highlights the four general principles which go to the "effective implementation" of the UNCRC, namely Article 2 (non-discrimination), Article 3(1) (best interests), Article 6 (inherent right to life and state obligations to ensure survival and development) and Article 12 (right to express views freely with those views being given due weight).

that safeguarding a child's right to data protection will inevitably have a negative impact on certain substantive rights under the UNCRC, for example, their right to freedom of expression or their right to play. It is worth noting in this regard that the UN Committee on the Rights of the Child has clarified that the best interests principle "is aimed at ensuring both the full and effective enjoyment of *all* the rights recognized in the Convention and the holistic development of the child[10]" (emphasis added).

It is the responsibility of organisations to assess the rights and position of child data subjects through the prism of not only the GDPR but the UNCRC and the best interests principle with a view to ensuring that the "specific protection" which the GDPR demands where an organisation is engaging in processing a child's personal data is fully implemented and that the organisation can demonstrate how the best interests principle has been given effect in light of the risks associated with the processing operations in question. Where organisations consider that there is a tension between the child's rights and position under the GDPR, and specific substantive UNCRC-based rights, the organisation must be able to demonstrate how in all the circumstances, the approach taken to the processing which gives rise to the perceived tension reflects the assessment and analysis of the best interests which has been carried out. In many cases, this will need to be based upon expert inputs and an evidence-based approach[11].

Commercial considerations aside, it is not clear to the DPC why there needs to be a trade-off between empowering and protecting children in the digital environment. It is possible to provide online services that empower children and are attractive to them but which also protect their personal data to the highest standards. The DPC recognises that embedding the best interests principle into online services in a truly holistic and meaningful manner will require significant efforts from members of the technology sector in particular, but organisations must accept that these additional accountability and compliance complexities are the price of doing business with children.

For all these reasons, the DPC is satisfied that no substantial changes need to be made to this section of the Fundamentals on the basis of the feedback received. However, the DPC is considering certain clarifying amendments to the text to reflect that the DPC understands that the best interests principle must involve an holistic and accountability-based assessment of all relevant circumstances including any other rights, as applicable, which the organisation may consider are engaged, through which the organisation can demonstrate how it has actually applied the best interests principle.

2.2 Legitimate interest and the "Zero interference" principle

The DPC received significant pushback from the technology sector on the "Zero interference" Fundamental. This principle involves online service providers that process children's data ensuring that the pursuit of legitimate interests does not interfere with, conflict with or negatively impact, at any level, the best interests of the child. Some

[10] ibid

[11] See for example paragraph 94 of UN Committee on the Rights of the Child General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*, which states: "*Children are a diverse group, with each having his or her own characteristics and needs that can only be adequately assessed by professionals who have expertise in matters related to child and adolescent development. This is why the formal assessment process should be carried out in a friendly and safe atmosphere by professionals trained in, inter alia, child psychology, child development and other relevant human and social development fields, who have experience working with children and who will consider the information received in an objective manner. As far as possible, a multidisciplinary team of professionals should be involved in assessing the child's best interests*."

submissions expressed the view that the DPC was suggesting Article 6(1)(f) could never be relied upon, that the DPC was going further than the legitimate interests balancing exercise set out under the GDPR and that the same balancing test should apply where children's data is concerned. It was also suggested that the DPC is proposing that no organisation's legitimate interest can prevail when children's data are processed.

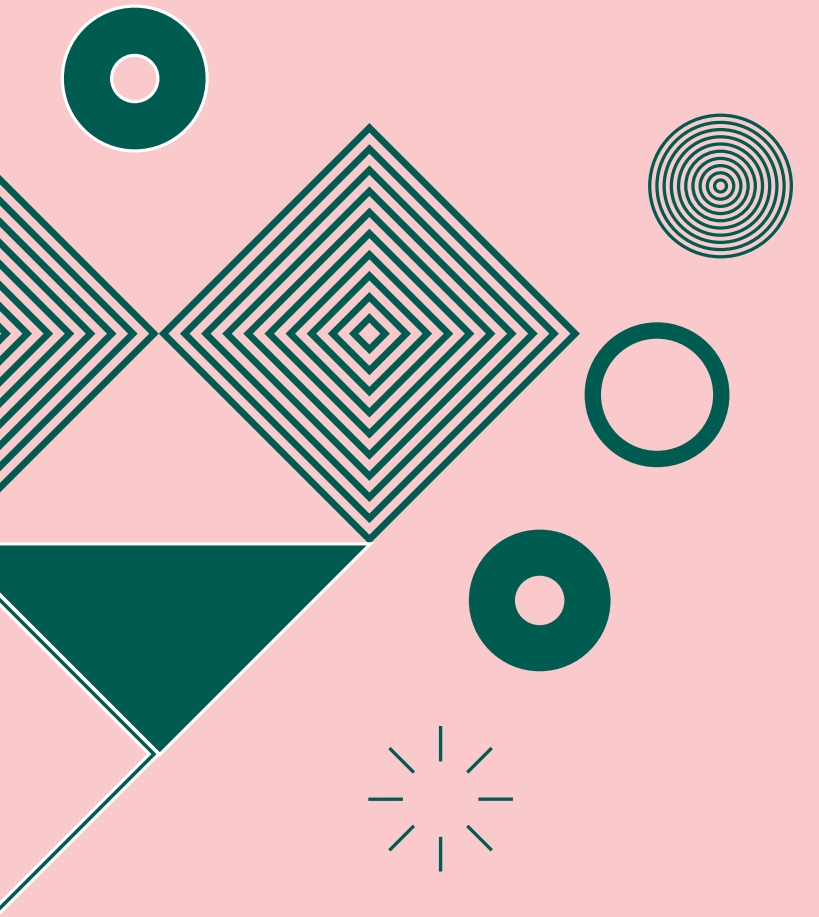
DPC response: As a preliminary point, the Fundamentals do not state that online service providers are excluded from relying on Article 6(1)(f) as a legal basis for processing children's data. Organisations may validly rely on this legal basis, where appropriate, provided they can demonstrate that their commercial interests do not negatively impact the best interests of the child at any level. The DPC does not consider that the same legitimate interests balancing test (i.e. where the position of adult data subjects is being considered) should apply where children's data is concerned, as this type of approach would completely ignore the explicit requirements in the GDPR that children merit specific protection and that organisations seeking to rely on Article 6(1)(f) should "in particular" have regard to the fundamental rights and freedoms of child data subjects. International and EU law make it manifestly clear that the best interests of the child should be paramount in any decision-making concerning the processing of children's data. In particular, this means that the interests and/ or fundamental rights and freedoms of child data subjects should always take precedence over the rights and interests of an organisation which is processing children's personal data for commercial purposes. While in general terms the legitimate interests legal basis allows for a certain, proportionate level of interference with the rights of data subjects, the balancing test inherent in this legal basis should be recalibrated where the data subjects are children. There seems to have been some confusion among certain stakeholders as to the meaning of "interfere with, conflict with" and "zero interference" (which some took to mean any (even positive) interference), however the DPC is satisfied that the text, as written, clearly indicates that this means a "negative impact".

Some organisations stated that the DPC has not accounted for scenarios where the legitimate interest of an organisation might negatively impact the best interests of a child but those negative effects could be mitigated. If organisations can demonstrate that they have mitigated the negative impact such that in the circumstances, there is no resultant interference with the child's best interests, then the effect of those mitigations would still be consistent with the zero interference principle.

Finally, concern was also expressed that the DPC's proposed approach to the legitimate interests balancing exercise may have the effect that their services could not be provided to child users, thereby depriving children of rich online experiences and opportunities to exercise their UNCRC-derived rights to freedom of expression and association, amongst others. The DPC considers that it is possible for service providers to remove potentially problematic elements of the processing from their services (at least when offered to child users) and thereby offer children a rich and empowering online service that does not threaten their fundamental rights and freedoms.

The purpose of the "Zero interference" Fundamental is not to prevent reliance on Article 6(1)(f) as a legal basis for processing but to ensure that where this legal basis is relied on, that organisations are carrying out meaningful and honest assessments of the risks and impacts upon child users and are truly putting the best interests of the child before their own commercial interests where the assessment requires this. If organisations design/ operate a business model which is at least in part dependent on carrying out processing

of children's data amongst its user population, then they must be willing to sincerely accept the additional obligations and responsibilities that this carries. Organisations who already claim that children's best interests are already at the heart of their service should be ready and willing to embrace this.



Transparency

3. TRANSPARENCY

In relation to transparency, the Fundamentals focus on three core principles: "Know your audience", "Information in every instance", and "Child-oriented transparency".

3.1 Know your audience

The Fundamentals emphasise that it is vital that organisations know who their audiences are, firstly so that they can assess whether they fall within the scope of the Fundamentals (Section 1) and also, so that they can tailor their transparency information for optimum accessibility and understandability. The DPC provides a number of examples of how this can be done, such as "conducting user testing, market research, user consultation and artificial intelligence (AI) amongst other things"[12]. Some submissions were concerned that this list was too prescriptive and felt that it should be up to the service to decide which specific method is the most appropriate. Concern was expressed about the DPC's suggestion of AI as a possible example of how an organisation might ensure they "know their audience" and considered that this could be interpreted as a positive affirmation of the use of AI as a tool to profile children and their needs and interests. The view was also expressed that it would be impossible to "know your audience" without collecting additional identification data which it considered runs counter to the principle of data minimisation.

DPC response: The list of methods provided by the DPC that can be implemented so that organisations "know their audience" at Section 1.3 are merely suggestions and – as is explicitly stated in the Fundamentals – is not exhaustive. Organisations are best placed to determine the method most appropriate to their service to use for these purposes and are not required to use one of the examples suggested by the DPC.

In relation to the DPC's reference to AI, this is a passive reference and not made for the purposes of actively either encouraging or discouraging the use of AI for the purposes of an organisation's assessment of its audience or for age verification purposes. However, the DPC is considering the addition of further guidance in the Fundamentals addressing the use of AI for identifying child users.

In any event, the DPC does not accept the assertion that requiring an online service provider to know its audience entails the collection additional identification data and therefore runs contrary to the principle of data minimisation. There is no requirement on controllers to collect hard identifiers for the purposes of ascertaining who their audience is. The DPC has already provided a number of examples of ways in which this could be achieved, but ultimately it is for organisations to be accountable and to be confident in the knowledge that they are providing appropriate transparency information to their users, particularly where those users are children. The citing of data minimisation as a reason for objecting to certain aspects of the Fundamentals also occurred in relation to age verification, and is dealt with further in Section 5.2 of this document.

[12]Section 1.3

3.2 Provide clear explanations of user control choices and default settings

The Fundamentals recommend that organisations should provide clear explanations of user control choices and default settings, and should provide explanations to children as to why certain settings are automatically switched to off or denied to them by default. The view was expressed that this requirement goes beyond the obligations of a data controller under the GDPR. Conversely, while there was also acceptance that this requirement supports a fully transparent approach to product design, a request was made that the DPC provide further guidance on how an organisation might comply with this requirement in a manner which does not also encourage child users to seek to circumvent such measures in order to attempt to gain access to any restricted/denied features (anticipating that organisations could run into difficulty when attempting to balance these two conflicting positions).

DPC response: The DPC considers that a critical component of the data protection by design and default obligation which applies to all organisations who act as data controllers, is that the personal data protective measures which should be built into the architecture of any online service must include granular privacy-enhancing controls and choices for children as a default. As part of compliance with its transparency obligations, therefore, an organisation should generally provide explanations to children as to why certain settings are automatically switched to off or denied to them by default. However the DPC is considering the broader point raised about the balance between transparency measures for denial/ blocking of certain adult user features and the risks of circumvention of such measures that might arise in certain cases and will address this in the finalised Fundamentals.

Exercising children's rights

4. EXERCISING CHILDREN'S RIGHTS

The Fundamentals emphasise that children are rights holders and, as such, should be permitted to exercise their own data protection rights at any age, provided they have the capacity to do so and provided it is in their best interests.

4.1 The age of children

Some submissions endorsed the DPC's approach to the removal of all barriers or unnecessary obstacles for children in exercising their rights, and welcomed the DPC's starting position that children of any age can, in principle, exercise their own rights. That said, a number of submissions touched on the issue of the varying needs of younger children and teenagers. One submission stated that there is an important distinction between young users and teenagers, and setting of age ranges by the DPC would help industry to understand when children might require assistance from their parents to exercise their rights and when they are considered to be of an age where they can do so independently. Another expressed the view that the Fundamentals should highlight the importance of service providers respecting the developing autonomy of young people, and should avoid requirements that have the effect of treating older children as lacking capacity. A further submission stated that, for the purposes of children exercising data protection rights, by not setting a specific age threshold, the Fundamentals make it difficult for organisations to implement in practice and instead place the burden on online service providers and will prove a barrier to compliance.

DPC response: The DPC considered the issue of setting age ranges and thresholds very carefully when drafting the Fundamentals. Based on feedback from children themselves, expert adult stakeholders, as well as extensive analysis of international law, it became clear that, given that there can be considerable variation in the cognitive development in children of the same age, particularly in early adolescence, it would be inappropriate, and indeed run counter to the principles of the UNCRC to set the sort of hard age-specific demarcations for the exercise of rights that certain submissions called for. In this regard, it is of critical importance that the UN Committee on the Rights of the Child, in its General Comment on the right of the child to be heard[13], directs that States should protect the right to be heard for every child capable of forming their own views and that the starting point should be a presumption of capacity on the part of a child to form their own views and the recognition that they have a right to express them. The UN Committee on the Rights of the Child also emphasises that the right to be heard as protected by Article 12 UNCRC has no age limit restricting the right of a child to express their views and it discourages States from introducing age limits in law, or practices, which would restrict the child's right to be heard in all matters affecting them. The DPC is concerned that by being prescriptive with age ranges and stipulating that a child, for example, between certain ages should not be able to submit an access request without the assistance of a parent or guardian, would be in contravention of the UNCRC. Likewise, imposing a hard cut-off in age above which a child should be able to submit an access request or an erasure request does not take account of the many scenarios in which it may not be in a child's best interests to do so, for example to provide access to personal data that has the potential to cause significant distress to

[13]General Comment No. 12 (2009) The Right of the Child to be Heard - see paragraph 20 - 21

the child. For these reasons, the DPC is satisfied that the approach currently taken in the Fundamentals is the most appropriate one. The list of criteria to be taken into account that the DPC provides for organisations when considering whether or not to acquiesce with a request from a child should give organisations a solid starting point when it comes to putting the Fundamentals into practice. With regard to perceptions that the DPC has burdened organisations by not identifying hard age thresholds, the DPC would highlight that it is not the role or responsibility of regulators to set such thresholds or to seek to implement measures that obviate controllers' clear GDPR obligations, including those arising particularly under Article 24, with regard to processing of children's data, to have regard to the varying likelihood and severity of risks posed by such processing, as well as accountability obligations. As mentioned earlier, if organisations make a conscious choice to process (and thereby to derive a benefit from such processing of) children's personal data, they must meaningfully accept and take on the challenges and additional obligations that come with this commercial choice.

With regard to the view that the Fundamentals contain requirements that may have the effect of treating older children as lacking capacity, the DPC would highlight that its intention is not to assume that older children lack capacity, in fact, quite the opposite. Rather the starting point, as set out in the Fundamentals is that children of all ages should be able to exercise their own rights, provided they have the capacity and provided it is in their best interests to do so.

4.2 Assessing capacity

Some submissions expressed doubt in relation to the capability of data controllers to assess the capacity of child users when it comes to decision-making involving the exercise of children's data protection rights. It was suggested in this regard that such decisions are best made by the child's parents or legal guardians as they are the ones who know the child best.

DPC response: The DPC acknowledges that the carrying out of best interests and capacity assessments by organisations will require additional resourcing and expert teams in place to carry out this work (as highlighted by UN Committee on the Rights of the Child in their General Comment No. 14). This is an inherent aspect of the additional obligations which will apply to organisations which choose to process children's data i.e. as an inevitable consequence of the decision to provide services to children. Any organisation which processes personal data must equally give effect to the exercise of data subject rights. Therefore it is an unavoidable feature of processing children's personal data that the organisation doing so must be in a position to deal with the complexities arising in connection with the exercise of children's rights as data subjects (including assessments of capacity). Organisations should not be seeking to displace responsibility for their own GDPR responsibilities as data controllers onto parents/ guardians. It is for an organisation to decide, in all of the circumstances of a given case, how it is most appropriate to respond to a request to exercise the data subject rights of a child (whether that is made by the child themselves or by a parent/ guardian).

The DPC acknowledges that large-scale platforms with millions of users (be they adults or children) will likely rely upon automated tools for the purposes of enabling data subjects to exercise their data protection rights. In the case of child users, organisations

should have dedicated, clear and child-friendly user flows in place to facilitate children to exercise their rights. In many circumstances, these automated tools may be sufficient, however regardless of the age of a user, organisations must have adequate measures in place which provide suitable avenues of redress for data subjects should they have more specific or complex requests, or in circumstances where a parent/guardian is seeking to exercise their child's data protection rights on their behalf, in which case organisations will inevitably have to deal with some requests on a case-by-case basis.

The DPC considers that the requirement to assess the individual capacity of a child for the purposes of ascertaining whether they have the capacity (and it is in their best interests) to exercise their own data protection rights will likely be the exception to the rule, as opposed to the norm. However, it is imperative that organisations consider the circumstances where exceptions may arise which would call for individual assessments (i.e. non automated/ human involvement in the assessment) up front at the design stage of their user flows and take consideration of the nature of the personal data they are processing and assess whether, in general terms, it would be appropriate to deal with a child data subject in an automated manner through self-service tools.

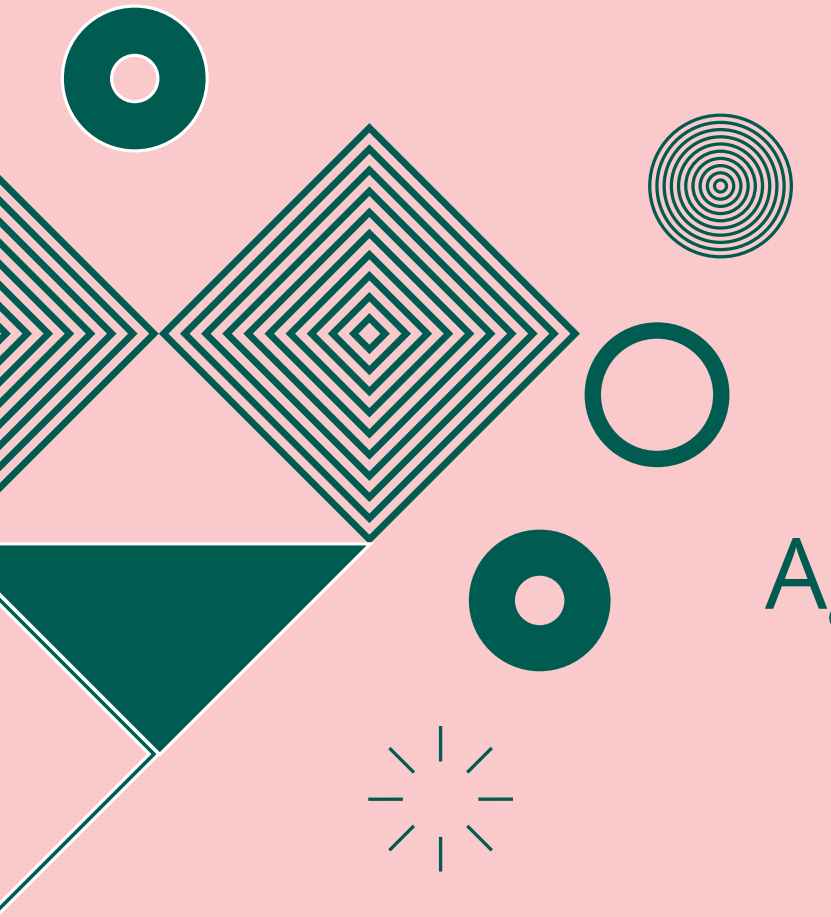
In general terms, the DPC considers that if an organisation deems it appropriate to engage with and offer services to child users above a certain age in the first place where the child user will generally autonomously interact with the service, those child users will likely be in a position to exercise their own data protection rights vis-à-vis that service/ organisation.

The DPC is considering the addition of further explanatory text around the issue of assessing capacity in the final version of the Fundamentals.

4.3 Acting on behalf of a child (verifying that someone is the guardian)

Some submissions also touched on the issue of acting on behalf children. The DPC's non-exhaustive list of factors was welcomed in the round, with some stakeholders requesting further guidance in this respect. One submission raised the issue of data minimisation again and how to verify that someone is really the parent/guardian of a child without excessively collecting information.

DPC response: Acting on behalf of another person (including a child) is not a concept particular to the GDPR / data protection and most organisations will have protocols in place for acting on requests which are made by, for example, legal representatives, next of kin, parties acting on foot of a power of attorney, or indeed parents/guardians. The principle of data minimisation should not be seen as a reason for an organisation not to comply with their controller responsibilities when it comes to issues such as verifying the age of children or the status of a parent or guardian as a holder of parental responsibility. As set out further below, the DPC does not consider that there is an incompatibility between undertaking such verification activities on the one hand, and complying with the principle of data minimisation on the other hand.



Age verification

5. AGE VERIFICATION

The topic of age verification attracted a wide variety of feedback and opinions from both the private and public sector. Among the issues raised were whether age verification is technically required under the GDPR and whether age verification simply leads to excessive data collection, thus infringing the principle of data minimisation. There were some requests for examples of what robust age verification mechanisms specifically look like, while other submissions called for the DPC not to be prescriptive in this regard. Some submissions sought practical guidance as to what services are deemed more likely to be high-risk processing situations to various ages of children, one submission requested more clarity about the expectations of age assurance in terms of its approach and qualities, while another sought further guidance and examples as to how organisations should adopt a risk-based approach to verification of parental consent. There was also a call for the DPC to explicitly acknowledge that age verification mechanisms that meet the standards required in the draft Fundamentals may not yet exist and that currently no age verification mechanism is perfect or free of risk. Another submission stated that the implementation of age verification mechanisms to distinguish adults from children across a wide range of online services would not currently be feasible for a number of technical, operational and legal reasons.

At the other end of the spectrum, submissions received from organisations in the age verification sector stated that effective means by which age-gating could be implemented on the Internet already exist and are fully operational when it comes to the sale of age-restricted goods and access to services such as gambling, and that thousands of such checks are made every day. It was suggested in one submission that it is impossible to apply the rights conferred on children by international and domestic law in the context of the internet, if they are not identified as children in the first place, and that "*age assurance is therefore, not an objective in its own right, but the basic foundation for the delivery of any rights or policies related to age*".

Another submission commented that many app developers and website providers claim that obtaining parental consent is a challenge and that the tools and technology are blockers to the user experience, and that "*this has led to some platforms turning a blind eye to the fact children are declaring older dates of birth in weak age gates to access services*". The submission expressed the view that these children must be protected and that platforms have a responsibility to acknowledge them and treat children appropriately.

DPC response: It is important to highlight that the Fundamentals clearly emphasise that, in the case of mixed audience platforms, if reliable and robust ways of assessing the age of a user cannot be implemented, controllers must show they have defaulted back to a floor of clear protections for **all** users in order to guarantee the specific protections **for children** that the GDPR anticipates. Taking a passive approach which emphasises the limitations of current technological solutions to verify age does not relieve controllers of the obligation to actively take meaningful steps to protect child users. The GDPR demands that controllers take special account of children. If children cannot be distinguished from other users, then controllers must ensure that all users benefit from a floor of protection so that the principles in these Fundamentals are applied to all processing of children's data.

5.1 An holistic approach to age verification

A number of submissions suggested that age verification should be viewed not as a single tactic, but rather as part of a collection of ongoing efforts that work dynamically to provide effective solutions. These organisations felt that age verification should viewed as one tool amongst a suite of other tools, such as data protection by design and default measures, that work to ensure age-appropriate online experiences.

DPC response: The DPC understands that there is no silver bullet when it comes to age verification and acknowledges this reality in the Fundamentals. We agree that not all situations will require the same level of verification and that many products and services may need a combination of age verification tools in order to ensure the most effective approach. For example, upfront age verification mechanisms such as age checks may only be the first stage in an organisation's age verification chain with it being followed by subsequent steps and interventions which are aimed at achieving a higher degree of confidence about the user's age.

The DPC cannot prescribe what methods are most appropriate for organisations because this will vary considerably from context to context, depending on a range of factors such as the type of personal data being processing and the level of risk associated with the processing of that personal data. However, whatever the combination of methods deployed, the result must be demonstrably robust and effective and achieve a level of reliability that is commensurate with the risks posed by the processing in question. The DPC is considering revisions to the section on age verification in the Fundamentals which would incorporate recently published research and literature on the topic.

5.2 Age verification and data minimisation

A number of submissions stated that the use of age verification might result in a large degree of upfront and potentially excessive collection of personal data, subsequently creating a tension with the requirements for proportionality and the principle of data minimisation.

DPC response: The DPC does not accept that there is an inherent conflict between data minimisation and the collection of personal data for the purposes for ascertaining the age of a user, and does not consider the principle of data minimisation to be an obstacle to age verification.

The principle of data minimisation requires an organisation to collect only the minimum information required to achieve its purpose. When it comes to processing personal data for the purposes of verifying the age of users, there should be no issue with an organisation doing so from a data minimisation perspective, provided the organisation only collects the data necessary in order to be able to achieve the requisite degree of certainty about the age of its users i.e. that which is proportionate to the level of risk arising from the processing of personal data. The principle of data minimisation

needs to be considered in this context alongside the equally important principles of purpose limitation and storage limitation. This means that personal data collected for the purposes of verifying age is not used by the organisation for any other purpose (which may entail keeping it separate from other personal data sources which may be used on an ongoing basis e.g. for the ongoing provision of services) and that the personal data collected which provides the basis for the age verification process to be undertaken is deleted once the appropriate level of confidence as to user age has been reached. The DPC is considering the addition of further text to address these issues in the final version of the Fundamentals.

Profiling, direct marketing and advertising

6. PROFILING, DIRECT MARKETING AND ADVERTISING

A number of submissions voiced concerns variously that the DPC, through Fundamental No. 12 ("Prohibition on profiling"), is imposing a blanket prohibition on profiling; that the Fundamentals imply that profiling is never in the best interests of the child; and that the DPC is significantly exceeding the limits of the GDPR, as well as approaches taken by other DPAs, such as the ICO. On the other hand, some submissions strongly supported the DPC's position on profiling, welcoming the robust prevention of advertising and the commercial targeting of children and stating that it is critical that children are protected from a complex advertising technology ecosystem.

6.1 Criticisms that the DPC approach involves an outright prohibition which exceeds the limits of the GDPR

DPC response: The assertion that the DPC is imposing an outright ban on profiling is incorrect. The draft Fundamentals clearly state[14] that online service providers should not profile children and/ or carry out automated decision-making in relation to children, or otherwise use their personal data, *for marketing/advertising purposes, unless they can clearly demonstrate how and why it is in the best interests of the child to do so*. This restriction on profiling pertains to the specific context of marketing and advertising. Even then, if online service providers can demonstrate that this profiling is in the best interests of the child, there is no reason, in principle, why they cannot proceed. It is for controllers to demonstrate how this may be the case. However, the DPC understands that there may be some sensitivity regarding the title "Prohibition on profiling", and so is considering linguistic edits to address this issue.

However, overall the DPC is satisfied that the current position as set out in the draft Fundamentals is consistent with the recent comment of the UN Committee on the Rights of the Child reflected in paragraph 42 of General Comment No. 25[15]. In fact, the UN Committee on the Rights of the Child goes further than the DPC in terms of the suggested approach to profiling, stating that profiling or targeting of children of any age **for commercial purposes** generally should be prohibited by State authorities:

> ***42. States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.***

[14]At page 7
[15]UN Committee on the Rights of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment. Available at: ***https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en***

The DPC also does not agree with the assertion made in some submissions that the DPC's position on this issue is more extreme than that of other data protection authorities, such the ICO. In its Age-Appropriate Design Code, the ICO cautions against the general profiling of children, stating that organisations must switch off by default any options within their service which rely on profiling, unless they can demonstrate a compelling reason why this should not be the case, taking account of the best interests of the child.

Meanwhile the Fundamentals address profiling in the specific context of *direct marketing and advertising* to children, and state that organisations should not profile children for these purposes, unless they can demonstrate that doing so is in the best interests of the child. The French data protection authority[16] follows a similar approach in its recommendations for protecting children online[17] in recommendation No.8 ("*Provide specific guarantees to protect the best interests of the child*") (unofficial translation), which states that data controllers should avoid profiling children because, even though if there is no absolute ban, the GDPR recitals, EDPB guidelines, and guidelines by other regulators such as the ICO and DPC all point towards a restriction on profiling of children except where it serves the best interests of children. Finally, the Dutch Data Protection Authority has adopted a similar position in its "Code for Children's Rights" in which it advises against the profiling of children unless there is an overriding reason in the best interests of the child.[18] Accordingly the DPC considers that its position on this matter is fully consistent with that of other data protection authorities.

[16]La Commission Nationale de l'Informatique et des Libertés (CNIL)
[17]See ***https://www.cnil.fr/fr/recommandation-8-prevoir-des-garanties-specifiques-pour-proteger-linter-et-de-lenfant*** (the above English translation was carried out by the DPC)
[18]See ***https://codevoorkinderrechten.nl/*** (In Dutch)

6.2 Profiling for the purposes of personalisation

Some submissions highlighted that the Fundamentals do not address the issue of profiling for non-advertising purposes, such as integrity and safety (which could be relevant to preventing children's access to harmful content) and personalisation, which some organisations commented could improve a child user's experience, for example by offering children a more focused, interesting and relevant website, ensuring a better experience for the child.

One submission recommended that the Fundamentals should further clarify what it considers as "marketing and advertising" in the context of the use of (for instance) recommendation engines which might be critical to the functioning of certain online services but which are not specifically engaging in marketing, e.g. recommendations of appropriate reading material for children.

Some organisations encouraged the DPC to pursue a risk-based approach to assessing the appropriateness of profiling for children and to clarify the scope of the activities to which the "Prohibition on profiling" Fundamental applies.

DPC response: The DPC acknowledges the calls for further clarification with regard to profiling for non-advertising purposes and will consider this in the context of finalising the Fundamentals.

6.3 Profiling and the best interests of the child

Some submissions expressed the view that the draft Fundamentals take a blanket approach that profiling and the best interests of the child cannot coexist. One submission suggested that the Fundamentals should acknowledge children's fundamental rights and freedoms including, but not limited to, children's autonomy, and should take a risk-based approach to profiling aligned with the GDPR.

DPC response: The DPC considers that profiling for marketing or advertising purposes will generally not align with the position that there should be zero interference with the best interests of the child in the processing of their personal data unless the organisation can demonstrate otherwise. As noted above, this is in line with the UN Committee on the Rights of the Child in their General Comment No. 25.

Tools to ensure a high level of data protection for children

7. TOOLS TO ENSURE A HIGH LEVEL OF DATA PROTECTION FOR CHILDREN

7.1 Data Protection by Design and Default measures

The DPC received a number of comments in relation to the section on Data Protection by Design and Default (DPDD) measures. One submission considered that the list of examples of DPDD measures provided by the DPC was too prescriptive, and that it was quite difficult to relate some of these measures to the 14 Fundamentals or to the rest of the content of the draft guidance. Another submission requested additional guidance and explanations about what types of data processing are considered to be detrimental and not in the best interests of children, highlighting that the DPC may wish to incorporate a similar approach to the one taken by the ICO in this regard.

Some submissions questioned the DPC's suggestion that the collection and processing of children's biometric data should be avoided, stating that some products require the processing of biometric data in order to operate and, in some cases, biometric technology can be useful to protect children. It was also highlighted that while processing on-device is encouraged, there are cases where it is not possible to process data on the device only.

One submission questioned the DPC's "default privacy settings" measure, stating that where a teenager makes a choice to change a default privacy setting, a requirement to "automatically switch it back to the default setting" at the end of the session would appear to conflict with other aspects of the Fundamentals, and that not respecting the user's choice would be in conflict with the Article 5 UNCRC requirement to take account of a child's evolving capacity.

The view was also expressed that a number of DPDD measures relate to parental controls or oversight and that while, in most cases, the Fundamentals acknowledge that this may not always be appropriate, some of the language suggests parental involvement will always be required regardless of the developmental capacity or age of the child (pointing to the measures on sharing and visibility and audience controls). The submission suggested that it would be helpful for the Fundamentals to clarify that these measures will not always be appropriate and to reiterate that the best interests of the child involves balancing the responsibilities, rights and duties of parents/caregivers to provide guidance in the exercise of a child's rights against the rights and capabilities of children exercising their own rights on their own behalf.

DPC response: Sections 7.1 and 7.2 of the Fundamentals provide important principles-based guidance as to the factors which organisations must consider when designing and evaluating their own settings, features, user choices, etc. The list of DPDD measures set out at Section 7.3 was explicitly stated to be a list of examples and an "indicative selection" and clearly not all such measures will be appropriate and/ or required in every specific scenario.

The DPC emphasises that what the GDPR requires is not rote adherence to a prescriptive list of measures but that organisations carefully examine the settings, features, user choices, etc. which form part of ***their own*** services from the perspective of their own

child users and carry out a meaningful and honest assessment of the real risks that might be posed to child users by replicating the same settings and features which are available to adult users.

Equally, organisations must take an holistic view of their services and processing operations to identify risky elements and to ensure mitigation or elimination of those risks. The DPC emphasises that it is not for it to direct service providers, especially in the digital sector, how to implement data protection by design and default, both from the ground up or on a rolling basis, whether in the case of child or adult users. Organisations are best placed to know the specificities of their own services and must combine this unique knowledge with appropriate expertise in the areas of design and child development and child protection, amongst others, when evaluating whether they have achieved meaningful compliance with their GDPR obligations, particularly those of data protection by design and default. In every case, it is for the organisation to be able to demonstrate how such a fulsome assessment has been carried out and why it has adopted the approach in question, whether that means choosing to apply a particular DPDD measure (which may be one of those included in the indicative list at Section 7.3 or not) or taking a decision not to apply a DPDD measure.

The DPC is considering what further clarifications may be needed to Section 7 in light of the above themes emerging from the submissions.

7.2 Data Protection Impact Assessments (DPIA)

Some submissions requested further guidance in relation to the topic of DPIAs and for the DPC to provide templates. There were also requests for guidance on how organisations might best utilise the best interests of the child as one of the primary risk evaluation tools when carrying out a DPIA, and on how organisations might demonstrate, from a documentation and accountability perspective, how the best interests principle has driven the design, development, implementation and/or operation of their service.

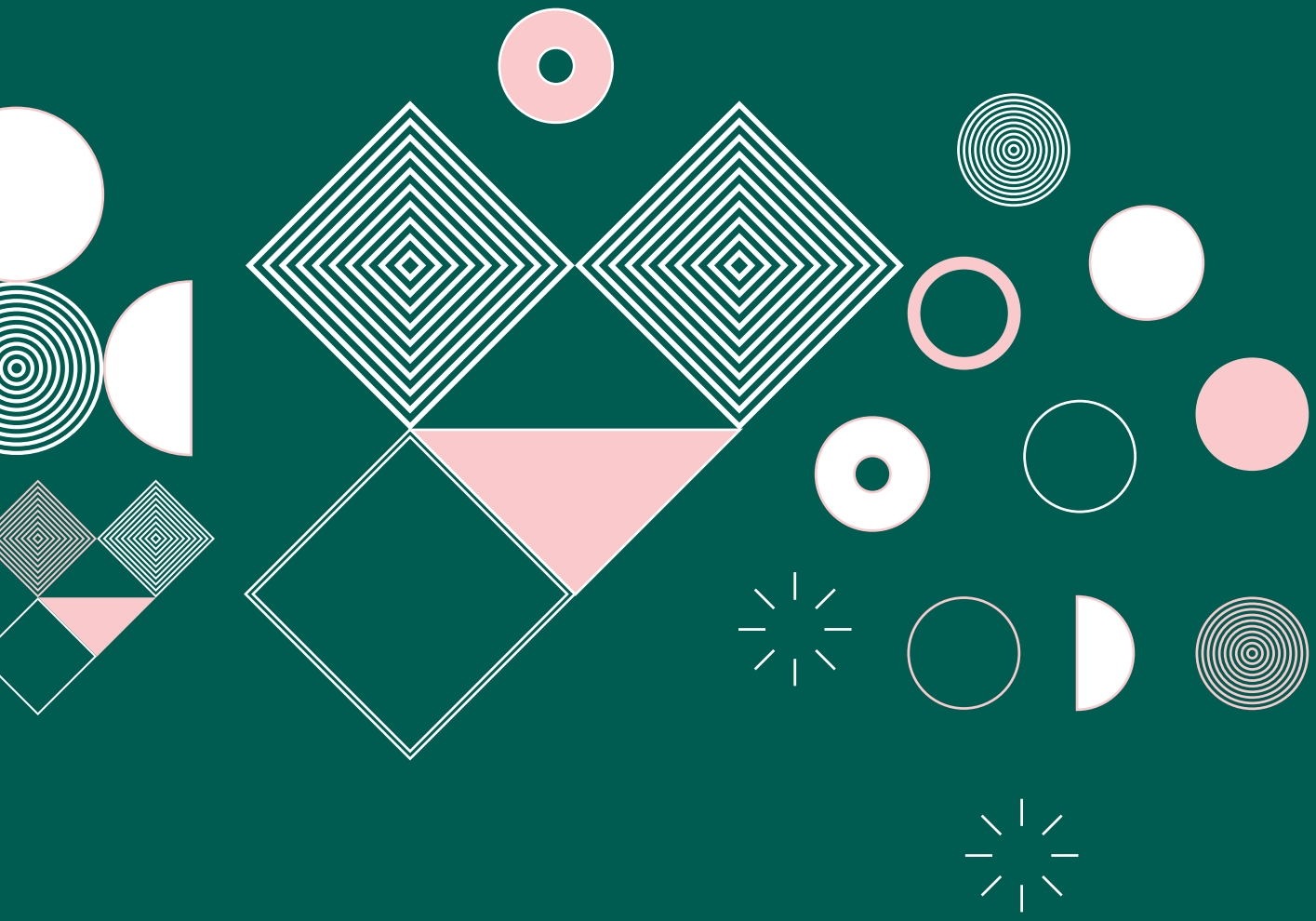
DPC response: Conducting DPIAs should already be commonplace for any organisation that processes children's personal data, and issues such as the structure of a DPIA and how best to demonstrate and document which factors have been taken into account in a DPIA are basic elements of conducting a DPIA. When it comes to DPIAs that specifically assess processing operations involving children's personal data, the DPC considers it necessary that organisations consult with child development and child safety experts to ensure they have considered the cumulative risks that could potentially be posed to children as part of their processing operations. The DPC is considering the addition of further text in the final version of the Fundamentals in light of the comments above.

Next steps

8. NEXT STEPS

The DPC is currently finalising the draft Fundamentals with a view to publication of the final version in late 2021.

As noted earlier, upon publication in final form, the Fundamentals will have immediate effect and there will be no lead-in period for compliance.



An Coimisiún um Chosaint Sonraí
Data Protection Commission
www.dataprotection.ie

An Coimisiún um Chosaint Sonraí
21 Cearnóg Mhic Liam, BÁC 2,
DO2 RD28, Éireann.

Data Protection Commission
21 Fitzwilliam Square, Dublin 2,
D02 RD28, Ireland