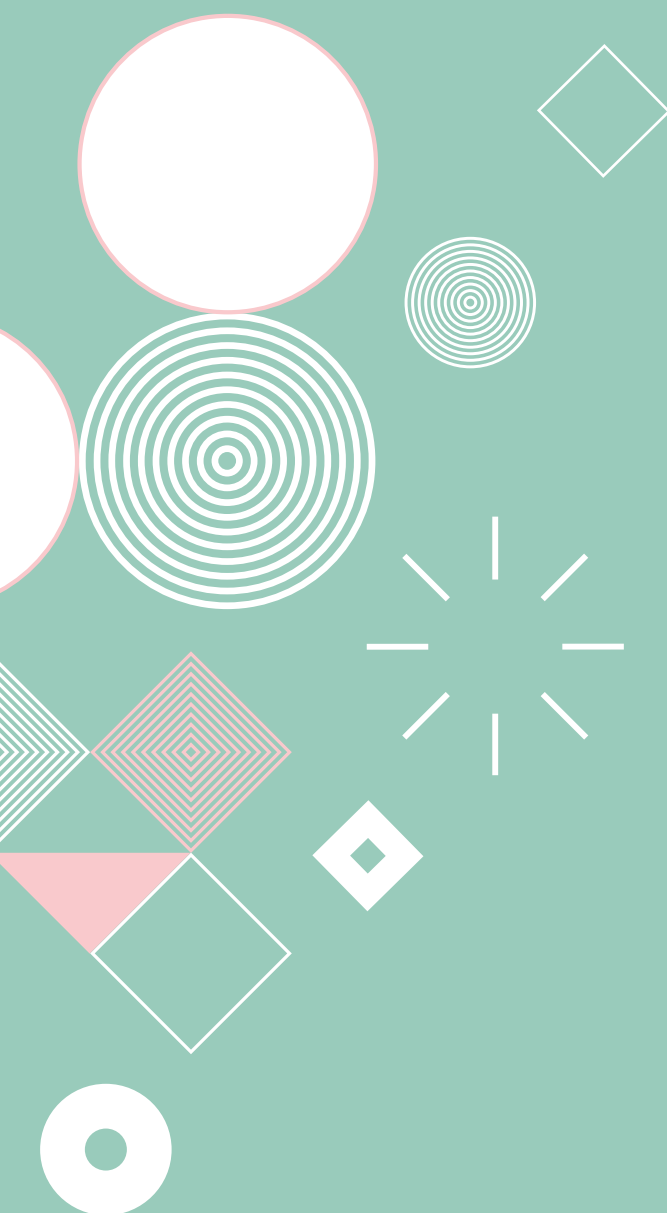


CHILDREN FRONT AND CENTRE



FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING

Draft Version for Public Consultation



Foreword

Foreword by the Commissioner for Data Protection

Insights derived from personal data are often described nowadays as the “new gold”. Hardly an organisation exists today that doesn’t have some form of web presence that tracks, traces and measures our engagement with it in order to better target us, whether for commercial or other purposes. About a quarter of Ireland’s population are children, all of whose personal data is processed every day online and offline, in educational, health, recreational and sporting, social services, and commercial contexts. It is with this in mind that the Data Protection Commission (DPC) has produced this guidance (the “Fundamentals”) to set out the standards that all organisations should follow when collecting and processing children’s data. The core message of these Fundamentals 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.

The General Data Protection Regulation (GDPR), which became applicable as a law on 25 May 2018, recognised for the first time in EU data protection law the specific circumstances and risks posed to children when their personal data is collected and processed without adequate safeguards. The GDPR emphasises the need for clear communication with children around how their personal data is processed when services are being targeted at them and points out that children may be less aware of the risks involved. In addition, it recognises the right of children to exercise their data protection rights, for example to have their personal data erased by online services so that they are not burdened in adulthood with decisions they made around their personal data when they had less understanding of the consequences of sharing their data in the digital environment.

In order to flesh out the higher standards of protection the GDPR requires for processing children’s personal data, the DPC as a priority engaged in a detailed public consultation in 2019 around the key issues relating to children’s personal data to seek a wide variety of stakeholder views which would inform how the DPC ultimately went about providing greater clarity to organisations which process children’s personal data, as well as parents and children themselves. In line with the UN Convention on the Rights of the Child, it was critically important for the DPC to consult directly with children on their data protection rights and to have their views heard and discussed. The feedback we gathered both from the direct consultation pilot workshops we ran with schools and then from the teachers who participated in our consultation with their classes has been invaluable to our understanding of both the views of children and the issues at play. We are indebted to all of those schools, principals, teachers and children who generously shared their feedback. Overall we had a high level of engagement in the consultation from children’s rights bodies, industry,

public sector organisations and children themselves.

In preparing this “Fundamentals” guidance on foot of our consultation, the DPC also had the opportunity to engage with an array of expert stakeholders in Ireland and also globally, many of whom contacted us proactively when they heard about this work and because they are committed to better protection of children particularly in online environments. We are very grateful for their continued support and engagement. While we have been completing this piece of work, our UK counterpart, the Information Commissioner’s Office (ICO) has produced an Age Appropriate Design Code for online services processing children’s data, as mandated by the UK Data Protection Act 2018 and that Code has now been approved by the UK Parliament. The focus of the ICO’s Code is on the necessary privacy-by-design features that must be engineered from the outset into services used by children. The focus of the DPC’s “Fundamentals” is somewhat broader in that it is not focused solely on the engineering and design of online products and services. Nevertheless, it is worth pointing out that the “Fundamentals” are entirely consistent with the UK Code and in particular it is clear that the best interests of the child principle underpin both.

It’s clear that the internet poses particular challenges when it comes to children’s data and there aren’t necessarily clear-cut answers about what is “right” or “wrong” in every case. For example, in the run up to the implementation of the Data Protection Act 2018 (the 2018 Act) (which gives further effect in Irish law to the GDPR), we witnessed in Ireland a particularly engaged and detailed debate at parliamentary level around the setting of the so-called “age of digital consent”, the age at which children should be able to consent to the processing of their personal data in an online context without parental involvement. The GDPR leaves it to the Member States to decide whether that age should be 13, 14, 15 or 16 years of age. What was interesting to see is that many child protection bodies, including statutory bodies, submitted that Ireland should set the threshold at the lowest age of 13 in order to protect the autonomy of teenagers and to ensure they were not impeded from accessing information services independently of their parents as they start to discover and explore their own identities. Academics and a number of politicians argued the age must be 16 in order to protect children from themselves and that their parents must be involved in supervision up to this point. Ireland ultimately selected 16; many other EEA Member States set it at 13 and a few others opted for 14 or 15. The Irish age of digital consent is due to be reviewed by the Minister for Justice, with that review to start no later than May next year and to be completed by May 2022.

Further complexities in terms of the internet relate to the range of online harms to which children can potentially be subject such as online bullying or exposure to harmful or illegal content, although these are outside the scope of

what is regulated by the GDPR. Some of the issues that have now manifested with the internet date back to the original open and democratic (rather than regulated and balkanised) philosophy behind the global internet which, it is now recognised, fails to distinguish between users of different, and in the case of children, evolving capacities. Jurisdictions all over the world have struggled with effective means by which age-gating could be implemented on the internet with many observers pointing out that age, in and of itself, is too blunt an instrument by which to measure capacity.

The “free” nature of the internet poses additional challenges as many services have evolved in such a way as to be free-of-charge to internet users but funded by behaviourally targeted advertisements that rely on tracking and profiling each of us as users. In our guidance, the DPC is clear that children’s personal data should not be collected in order to profile them and target them with advertisements. Such a policy should be easily implemented on services that target children specifically but becomes considerably more complex in “mixed use” internet environments. In such circumstances, service providers must have means of identifying and protecting children on their platform or else must implement a no-profiling policy across the board. The issue of contextual advertising (which doesn’t rely on using personal data but rather delivers advertisements based on on-screen content) to children on child-focused online services is beyond the scope of data protection law. Many parents object to the idea of children being targeted with, for example, fast food advertisements on online sites. However such contextual advertising needs to be regulated through advertising standards rather than the GDPR as these advertisements aren’t tailored based on personal data. Interestingly when the DPC consulted directly with children, we found many raised with us the idea of trade-offs between a free internet where they are tracked versus a subscription-based internet and some told us “It’s better than paying!”

Offline contexts too are important when it comes to the processing of children’s data and the DPC’s guidance looks at the issues of when children should be entitled to exercise their various data protection rights to access, erasure and restriction of processing independently of their parents. It is clear this is an area very much linked to the evolving capacity of the child and requires a careful balancing of where the best interests of the child lie.

These “Fundamentals” are now being published for a final round of consultation and we are keen to hear from any interested parties that wish to make submissions to us on any aspect of the document until the end of March 2021. In particular, we would be very pleased to hear from our fellow EEA data protection authorities, as the standards we are setting for the global internet service providers established in Ireland will affect all child data subjects across the EEA.

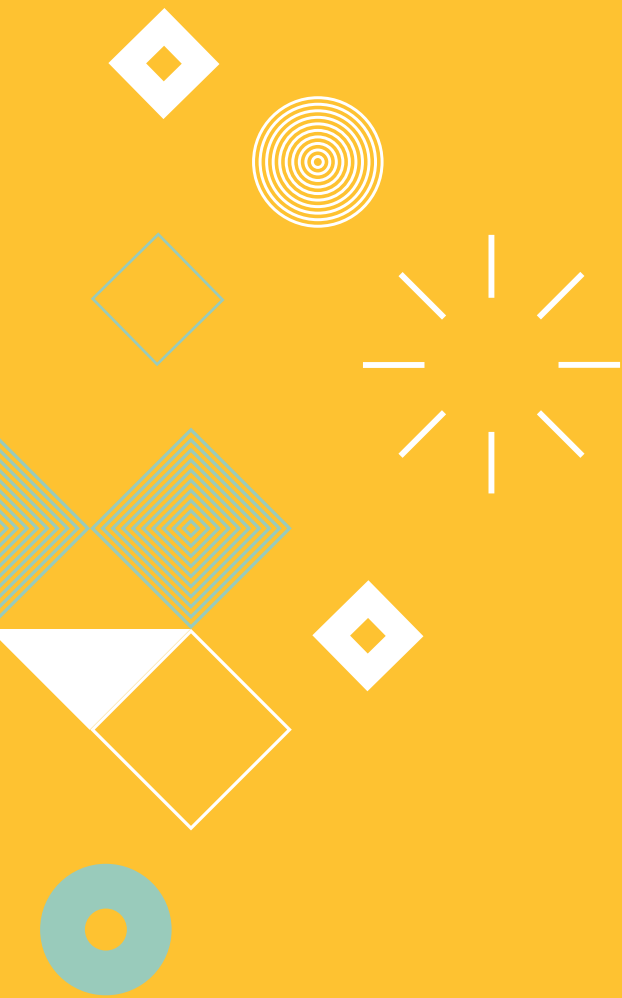
Beyond this consultation, the DPC is already preparing to engage fully with its Section 32 obligation under the 2018 Act to encourage the drawing up of Codes of Conduct for various sectors that process children’s data. On that basis, we would be very keen to hear from stakeholders across all sectors (e.g. internet service providers, social services providers, education sector providers etc.) that would be interested in engaging with the DPC in relation to a sectoral code of conduct with the aim of driving the higher standards of protection for children’s personal data required under the GDPR and creating a level playing field within sectors.

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.

Thank you for reading and for your continued engagement.

Helen Dixon

Commissioner for Data Protection
Data Protection Commission, Ireland



Executive Summary

The Fundamentals for a Child-Oriented Approach to Data Processing (the Fundamentals) have been drawn up by the Data Protection Commission (DPC) to drive improvements in standards of data processing. They introduce child-specific data protection interpretative principles and recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their use of/ access to services in both an online and offline world. In tandem, the Fundamentals will assist organisations that process children’s data, by clarifying the principles, arising from the high-level obligations under the GDPR, to which the DPC expects such organisations to adhere.

This version of the Fundamentals is published for the purpose of consulting with all interested parties. Observations and submissions on these Fundamentals can be made to the DPC by 31 March 2021. Further details on the consultation process can be found at Section 8. Following the conclusion of the DPC’s consultation process, a final version of the Fundamentals will be published which will inform the DPC’s approach to supervision, regulation and enforcement in the area of processing of children’s personal data.

The term “Fundamentals” has been used to illustrate the critical nature of these standards and expectations. Both online and offline (where applicable), the Fundamentals should be complied with by all organisations processing children’s data. This includes services that are directed at/ intended for, or are likely to be accessed by children.

In Ireland, for data protection purposes, a child is somebody under the age 18¹, in keeping with the definition of a child under the UN Convention on the Rights of the Child (UNCRC) as “a person under the age of 18 years.”

The DPC has identified the following 14 Fundamentals that organisations should follow to enhance protections for children in the processing of their personal data:

1. **FLOOR OF PROTECTION:** Online service providers should provide a “floor” of protection for all users, unless they take a risk-based approach to verifying the age of their users so that the protections set out in these Fundamentals are applied to all processing of children’s data (Section 1.4 “Complying with the Fundamentals”).
2. **CLEAR-CUT CONSENT:** When a child has given consent for their data to be processed, that consent must be freely given, specific, informed and unambiguous, made by way of a clear statement or affirmative action (Section 2.4 “Legal bases for processing children’s data”).
3. **ZERO INTERFERENCE:** Online service providers processing children’s data should ensure that the pursuit of legitimate interests do not interfere with, conflict with or negatively impact, at any level, the best interests of the child (Section 2.4 “Legal bases for processing children’s data”).
4. **KNOW YOUR AUDIENCE:** Online service providers should take steps to identify their users and ensure that services directed at/ intended for or likely to be accessed by children have child-specific data protection measures in place (Section 3.1 “Knowing your audience”).
5. **INFORMATION IN EVERY INSTANCE:** Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data (Section 3 “Transparency and children”).

-
6. **CHILD-ORIENTED TRANSPARENCY:** Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child (Section 3 “Transparency and children”).
 7. **LET CHILDREN HAVE THEIR SAY:** Online service providers shouldn’t forget that children are data subjects in their own right and have rights in relation to their personal data at any age. The DPC considers that a child may exercise these rights at any time, as long as they have the capacity to do so and it is in their best interests. (Section 4.1 “The position of children as rights holders”)
 8. **CONSENT DOESN'T CHANGE CHILDHOOD:** Consent obtained from children or from the guardians/ parents should not be used as a justification to treat children of all ages as if they were adults (Section 5.1 “Age of digital consent”).
 9. **YOUR PLATFORM, YOUR RESPONSIBILITY:** Companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/ or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and verification of parental consent are effective. (Section 5.2 “Verification of parental consent”)
 10. **DON'T SHUT OUT CHILD USERS OR DOWNGRADE THEIR EXPERIENCE:** If your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience. (Section 5.4 “Age verification and the child’s user experience”)
 11. **MINIMUM USER AGES AREN'T AN EXCUSE:** Theoretical user age thresholds for accessing services don't displace the obligations of organisations to comply with the controller obligations under the GDPR and the standards and expectations set out in these Fundamentals where “underage” users are concerned. (Section 5.5 “Minimum user ages”)
 12. **PROHIBITION ON PROFILING:** 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 due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so (Section 6.2 “Profiling and automated decision making”).
 13. **DO A DPIA:** Online service providers should undertake data protection impact assessments to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their personal data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests (Section 7.1 “Data Protection Impact Assessments”).
 14. **BAKE IT IN:** Online service providers that routinely process children’s personal data should, by design and by default, have a consistently high level of data protection which is “baked in” across their services (Section 7.2 “Data Protection by Design and Default”)

The DPC, having examined in detail the additional protections required under the GDPR



in relation to child users, has identified **a number of practical recommended measures** (see Section 7.2) to create safer, more appropriate and more privacy-respecting online environments for children to play, interact, learn and create than currently exists.

The DPC notes that complying with an age-appropriate/child-oriented regime of data protection will involve costs and take creativity on the part of service designers, however, children are one in three users, and represent the adult market of the future. A healthy and supportive relationship with children is therefore, in the long-term, to the benefit of brands and businesses across all sectors.



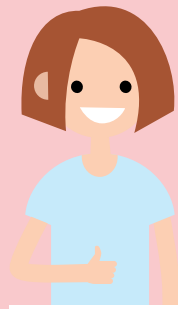
Foreword by the Commissioner for Data Protection	2
Executive Summary	5
1. Introduction	11
1.1 Children and the GDPR	12
1.2 The Fundamentals	13
1.3 Organisations that should comply with the Fundamentals	15
1.4 Complying with the Fundamentals	16
1.5 Recommended measures to support compliance with the Fundamentals	16
2. The landscape of children's rights	17
2.1 Legal backdrop	18
2.2 The best interests of the child	19
2.3 Rights and protections for children in the GDPR	20
2.4 Legal bases for processing children's personal data	21
3. Transparency and children	25
3.1 Knowing your audience	26
3.2 Methods to convey transparency information to children	28
4. Exercising children's data protection rights	31
4.1 The position of children as rights holders	33
4.2 Acting on behalf of a child	35
5. Age of digital consent and age verification	38
5.1 Age of digital consent	39
5.2 Verification of parental consent	39
5.3 Age verification purposes	41
5.4 Age verification and the child's user experience	42
5.5 Minimum user ages	43
5.6 Age verification mechanisms	43
5.7 Criteria for a risk-based approach to age verification	44
6. Direct marketing, profiling and advertising	46
6.1 Direct marketing	47
6.1.1 Legitimate interests and direct marketing	48
6.1.2 GDPR right to object to marketing	49
6.1.3 Consent for marketing to children	49





6.2	Profiling and automated decision making	51
6.2.1	User profiles and tracking technologies	52
6.2.2	Adtech	54
6.2.3	Can organisations use children's personal data to profile them and make automated decisions about them?	54
7.	Tools to ensure a high level of data protection for children	56
7.1	Data Protection Impact Assessments	57
7.2	Data Protection by Design and Default	58
7.3	Recommended measures for incorporating data protection by design and by default to promote the best interests of child users	59
8.	Conclusion	63
	Consultation Process	64
	Notes	65
	Appendix 1 – Glossary of terms	71
	Appendix 2 – Articles and recitals referenced in the Fundamentals relevant to the specific protection of children in the GDPR	74





Introduction

1. INTRODUCTION

We live in an age where vast amounts of information about us are collected, stored, used and shared by countless organisations – and much of the time this happens without our knowledge, particularly when we engage in online activity. Entry into the digital world now happens at a very early age with pre-school children frequently interacting with online organisations through the use of mobile phones, connected toys and other devices². This collection and use of each child’s personal data, once it begins, will doubtless continue throughout their lifetime as they live their daily lives using online social media, communication, entertainment, information, shopping, banking and countless other services.

This document has been informed by the output of the two-streamed public consultation which the DPC ran during the first half of 2019. The objective was to give all stakeholders an opportunity to have their say on issues around the processing of children’s personal data, the specific standards of data protection applicable to children, and the rights of children as data subjects. One stream of this consultation was addressed directly to children and young people and encouraged them to consider and give their views on the use of their own personal data and their rights in a social media context. The other stream of the consultation was addressed to all other stakeholders including parents, educators and children’s rights organisations, as well as organisations which process children’s data. That stream of the consultation sought the views of stakeholders on a range of issues concerned with processing of children’s data. The DPC’s consultation materials for both streams of the 2019 consultation can be found on its website³ as can the DPC’s reports on the outputs from both streams of the consultation.⁴

1.1 CHILDREN AND THE GDPR

The General Data Protection Regulation (GDPR) is an EU law which became applicable on 25 May 2018. It is essentially a new set of data protection rules concerned with ensuring that each of us knows when personal information about us (personal data) is collected and how it will be used, and giving us more control over the use of our personal data. One of the most significant changes the GDPR has brought about is the new emphasis placed on the importance of protecting children’s personal data. Children are very much front and centre of the data protection landscape in Europe, with Recital 38 of the GDPR stating that children merit specific protection when it comes to the processing of their personal data because they may be less aware of the risks, consequences and safeguards involved as well as their data protection rights. Where children are aware of the risks associated with the processing of their personal data, their age, maturity and developmental capacity will impact on their ability to be able to mitigate those risks.

Since the GDPR is a principles-based law, the rules are set out in it in very broad terms. The GDPR does not generally address how those rules should be interpreted and applied in specific situations, including where children’s personal data is concerned. In Ireland, a further national law, the Data Protection Act 2018 (the 2018 Act) was passed to give further effect to certain aspects of the rules in the GDPR. While there are a small number of provisions in the 2018 Act which concern processing of children’s personal data, for the most part these do not elaborate on how the general rules in the GDPR should be applied where children are concerned.

It is important to highlight that these Fundamentals focus on child-specific provisions and so should not be taken to be the sum total of all obligations that apply under the GDPR. Rather, the Fundamentals should be read in conjunction with other guidance issued by the DPC.

1.2 THE FUNDAMENTALS

The Fundamentals of data protection for children are as follows:

1. **FLOOR OF PROTECTION:** Online service providers should provide a “floor” of protection for all users, unless they take a risk-based approach to verifying the age of their users so that the protections set out in these Fundamentals are applied to all processing of children’s data (Section 1.4 “Complying with the Fundamentals”).
2. **CLEAR-CUT CONSENT:** When a child has given consent for their data to be processed, that consent must be freely given, specific, informed and unambiguous, made by way of a clear statement or affirmative action (Section 2.4 “Legal bases for processing children’s data”).
3. **ZERO INTERFERENCE:** Online service providers processing children’s data should ensure that the pursuit of legitimate interests do not interfere with, conflict with or negatively impact, at any level, the best interests of the child (Section 2.4 “Legal bases for processing children’s data”).
4. **KNOW YOUR AUDIENCE:** Online service providers should take steps to identify their users and ensure that services directed at/ intended for or likely to be accessed by children have child-specific data protection measures in place (Section 3.1 “Knowing your audience”).
5. **INFORMATION IN EVERY INSTANCE:** Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data (Section 3 “Transparency and children”).
6. **CHILD-ORIENTED TRANSPARENCY:** Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child (Section 3 “Transparency and children”).
7. **LET CHILDREN HAVE THEIR SAY:** Online service providers shouldn’t forget that children are data subjects in their own right and have rights in relation to their personal data at any age. The DPC considers that a child may exercise these rights at any time, as long as they have the capacity to do so and it is in their best interests. (Section 4.1 “The position of children as rights holders”).
8. **CONSENT DOESN’T CHANGE CHILDHOOD:** Consent obtained from children or from the guardians/ parents should not be used as a justification to treat children of all ages as if they were adults (Section 5.1 “Age of digital consent”).
9. **YOUR PLATFORM, YOUR RESPONSIBILITY:** Companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/ or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and verification of parental consent are effective. (Section 5.2 “Verification of parental consent”).
10. **DON’T SHUT OUT CHILD USERS OR DOWNGRADE THEIR EXPERIENCE:** If your service is directed at, intended for, or likely to be accessed by children, you can’t bypass your obligations simply by shutting them out or depriving them of a rich service experience. (Section 5.4 “Age verification and the child’s user experience”).

-
11. **MINIMUM USER AGES AREN'T AN EXCUSE:** Theoretical user age thresholds for accessing services don't displace the obligations of organisations to comply with the controller obligations under the GDPR and the standards and expectations set out in these Fundamentals where "underage" users are concerned. (Section 5.5 "Minimum user ages")
 12. **PROHIBITION ON PROFILING:** 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 due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so (Section 6.2 "Profiling and automated decision making").
 13. **DO A DPIA:** Online service providers should undertake data protection impact assessments to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their personal data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests (Section 7.1 "Data Protection Impact Assessments").
 14. **BAKE IT IN:** Online service providers that routinely process children's personal data should, by design and by default, have a consistently high level of data protection which is "baked in" across their services (Section 7.2 "Data Protection by Design and Default")

These Fundamentals (the genesis of which are displayed in **yellow** throughout the text) set the marker for organisations that process children's data by establishing the baseline expectations of the DPC as the regulator in Ireland for the processing of children's personal data, and also as the lead supervisory authority (LSA) under the GDPR for multinational organisations whose main or single establishment in the EEA is in Ireland.

1.3 ORGANISATIONS THAT SHOULD COMPLY WITH THE FUNDAMENTALS

The DPC considers that organisations should comply with the standards and expectations which are established in these Fundamentals when the services provided by the organisation are directed at, intended for or likely to be accessed by children.

A service that is directed at/ intended to be accessed by children will generally be self-evident from the manner in which the service markets, describes or promotes itself. However, services which have mixed user audiences i.e. including children, may be less obvious. In this regard, “likely to be accessed by a child” means that this is more likely than not. Offline, this applies to educational providers, sports and social clubs and communities, and health and social support providers amongst others. In a digital context, this includes websites, apps and other internet-of-things services which provide social media, media sharing, gaming, entertainment, educational, advocacy, health and social care/ support services. Whenever an organisation’s services are directed at, intended for, or likely to be accessed by children, the organisation should ensure that child-specific data protection measures are in place to enhance the level of protection afforded to children against the data processing risks posed to them by their use of/ access to the service.

In line with the European Data Protection Board’s (EDPB) guidance on transparency⁵ and indeed consistent with the requirement under the GDPR to maintain records of processing activities⁶, organisations should “know” their users/ audience and have knowledge about the people they collect information about. This may be done for example through conducting user testing, market research, user consultation and artificial intelligence amongst other things. In addition, the following (non-exhaustive) factors assist in assessing whether a website, app or other online service is likely to be accessed by children⁷:

- the subject matter/ nature of the site or service;
- its visual content;
- the use of animated characters or child-oriented activities and incentives;
- music or other audio content;
- the age of models;
- the presence of child celebrities or celebrities who appeal to children;
- language or other characteristics of the website or online service;
- whether ads promoting or appearing on the website or online service are directed at children;
- the age of users on similar services; and
- independent research

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. Organisations, as data controllers, must ensure that children have the benefit of “specific protection” under the GDPR and this derives in part from Article 24 which requires that controllers must take into account the risks of varying likelihood and severity for the rights and freedoms of natural persons, and implement appropriate technical and organisational measures to ensure that processing complies with the GDPR. (See Section 7 and also Appendix 2 which sets out the provisions in the GDPR which reference the protections for children mandated under the GDPR and the corresponding higher standards which controllers must apply when processing children’s personal data.)




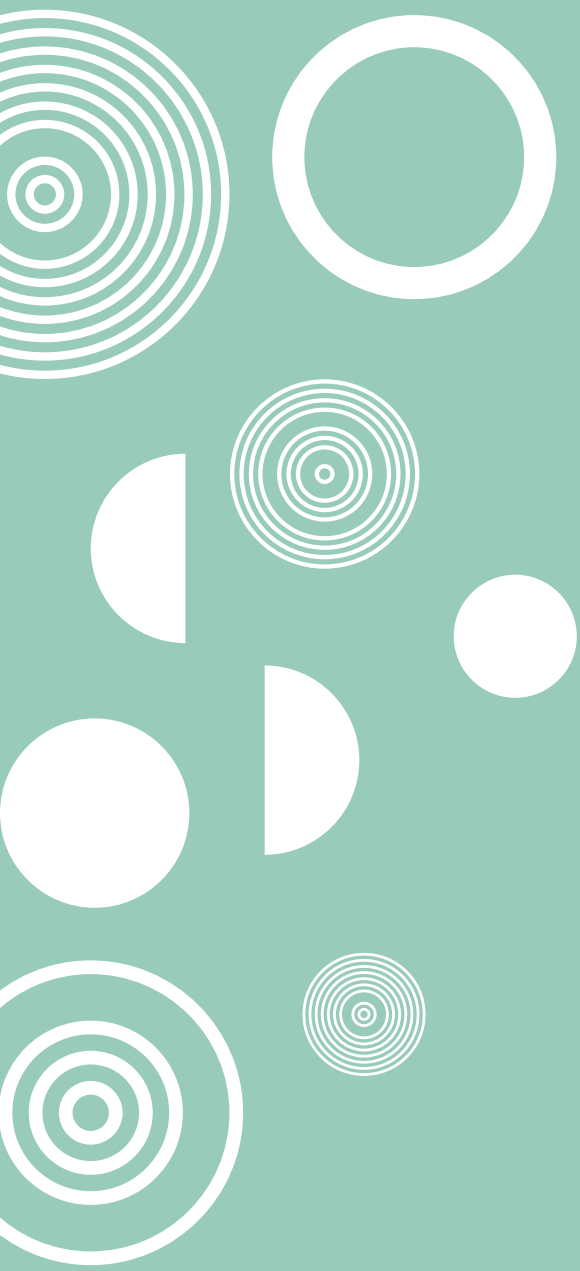
1.4 COMPLYING WITH THE FUNDAMENTALS

In essence, organisations have two choices. Either they can **apply the requirements of the Fundamentals to the services they offer holistically, so that all users (irrespective of whether they are under 18 or not) benefit from a high and standardised level of data protection sufficient to protect the rights of any child users.** Alternatively, if organisations choose not to apply a “floor of protection” for all their users which complies with these Fundamentals, then they should take a risk-based approach to verifying the age of their users so that they can ensure that they apply the requirements of these Fundamentals to the processing of their child users’ personal data. This approach is consistent⁸ with that taken by the ICO in its children’s code (the Age Appropriate Design Code⁹). Issues of age verification are considered in Section 6.

1.5 RECOMMENDED MEASURES TO SUPPORT COMPLIANCE WITH THE FUNDAMENTALS

The Fundamentals are designed to assist organisations that process children’s data by clarifying the principles arising from the high-level obligations under the GDPR to which the DPC expects such organisations to adhere. The DPC has set out a number of recommended measures that will support organisations in taking the practical steps necessary to comply with these Fundamentals and help them to demonstrate that they are implementing the high levels of protection required under the GDPR in the processing of children’s personal data. **These recommended measures are set out in detail in Section 7.2** and cover a range of data protection by design and default issues including default features and settings, transparency, tracking and profiling, user controls, parental oversight/ intervention, security measures and privacy-enhancing techniques.





The landscape of children's rights



2.1 LEGAL BACKDROP

In addition to the data protection rights and the protections for children set out in the GDPR, it is important to understand the wider legal backdrop to children's rights which informs how regulators, and ultimately the courts at national and EU level, interpret the legal rights and obligations relating to the processing of children's data under the GDPR.

Aside from the constitutional protection for children's rights in Ireland¹⁰, at European level, there are a number of legal instruments establishing rights of the child, including the 1996 Council of Europe Convention on the Exercise of Children's Rights¹¹ and the 2008 European Parliament Resolution titled "Towards an EU Strategy on the rights of the child"¹². However, the primary source, at an international level, of legal rights for children is the 1989 UN Convention on the Rights of the Child¹³ (UNCRC), which is the most ratified convention in history¹⁴. Having ratified the UNCRC in 1992, Ireland has an obligation under international law to respect, protect and fulfil the rights of children set out in the UNCRC.

In the context of children and data protection, some of the most relevant rights under the UNCRC include:

- Article 1 which defines a child as everyone under the age of 18 (unless the age of majority is lower under the applicable law) with each such person entitled to the rights in the UNCRC;
- Article 3 which requires that the best interests of the child must be a primary consideration in all actions, both public and private, concerning children and that all necessary care and protection should be ensured to protect their wellbeing;
- Article 5 which recognises that the responsibilities, rights and duties of parents and legal guardians to provide guidance in the exercise of the child's rights under the UNCRC must be consistent with the evolving capacities of the child (i.e. the child's developmental capacity);
- Article 8 which recognises the child's right to identity and that all aspects of identity must be protected and preserved;
- Article 12 which requires that any child who is capable of forming his or her own views has the right to express those views freely in all matters affecting them and that those views are given due weight in accordance with the child's age and maturity;
- Article 13 which provides for the child to have the right to freedom of expression including the freedom to seek, receive and impart information and ideas of all kinds;
- Article 14 which guarantees respect for the child's freedom of thought, conscience and religion; and
- Article 16 which secures the child's right to privacy, family and correspondence, echoing Article 8 of the European Convention on Human Rights¹⁵;
- Article 17 which recognises the child's right to access information from the media, from a variety of courses and that the child should be protected from materials that could harm them;
- Article 31 which recognises that every child has the right to relax, play and take part in a wide range of activities; and
- Article 32 which protects the right of the child against, amongst other things, economic exploitation.

2.2 THE BEST INTERESTS OF THE CHILD

Both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) have recognised the binding nature of the UNCRC, and the CJEU has held that the primacy of the interests of the child (the principle from Article 3 of the UNCRC) is the prism through which the provisions of EU law must be read.¹⁶

Separately, at an EU level, Article 3(3) of the Treaty on the European Union provides, amongst other things, for the protection of the rights of the child.¹⁷ Furthermore, the Charter of Fundamental Rights of the EU¹⁸ (the Charter) specifically recognises, at Article 24, the rights of children to have their views on matters which concern them taken into consideration in accordance with their age and maturity and for all public authorities and private institutions to make the child's best interests a primary consideration. The Charter, in its Explanations¹⁹, explicitly states that this article is based on the UNCRC.

The UN Committee on the Rights of the Child²⁰ (the UN Committee) has stated²¹ that determining what is in the best interests of the child should start with an assessment of the specific circumstances that make the child unique, and that the following elements should be taken into account when assessing the child's best interests:

- The child's views
- The child's identity
- Preservation of the family environment and maintaining relations
- Care, protection and safety of the child
- A situation of vulnerability
- The child's right to health
- The child's right to education

When it comes to balancing the various elements in the best interests assessment, the UN Committee considered that there may be situations where "protection" factors requiring restriction of the child's rights need to be assessed against the child's "empowerment" (e.g. the full exercise of their rights without restriction). In such situations, the UN Committee's position is that the age and developmental capacity of the child should be taken into account to assess the level of maturity of the child.

It is also noteworthy that the concept of the best interests of the child was explored by the predecessor to the EDPB²², the Article 29 Working Party, in its 2009 Opinion²³ in which it emphasised that the "*principle must be respected by all entities, public or private, which make decisions relating to children*". [emphasis added]. It is also notable that Recital 2 of the GDPR, while not specific in its application to children, underscores that the GDPR is intended to contribute to the well-being of natural persons.

Accordingly, it is clear that the obligation deriving from international and EU law to act in the best interests 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 DPC also notes that the UN Committee on the Rights of the Child is preparing a General Comment on Children's Rights in Relation to the Digital World²⁴, and will refer to it as part of this consultative process.

2.3 RIGHTS AND PROTECTIONS FOR CHILDREN IN THE GDPR

The GDPR is about empowering data subjects and giving them control over their personal data, including through their data protection rights, and children are no exception to this. It is important to note that the GDPR, while requiring extra protections for children, equally does not seek to deprive children of any of the rights which are enjoyed by (adult) data subjects.

The GDPR requires organisations to implement higher standards of protection when processing children's personal data (such as the requirement in Article 12(1) that controllers should take appropriate transparency measures when providing information on processing to a child, the specific references to children in Article 17 concerning erasure or the "right to be forgotten", and the indicators in Recital 71 that children should not be subject to profiling or automated decision-making). These types of additional obligations on organisations reflect the overarching approach of the GDPR towards children's personal data – found in Recital 38 – which is that **children merit specific protection with regard to their personal data as they may be less aware (i.e. due to their age, maturity and developmental capacity) of the risks, consequences and safeguards, and their rights in relation to the processing of their personal data.**

Separately, Recital 38 also stipulates that the rules concerning the age of digital consent should not prevent children from accessing online counselling or preventative services, meaning that children under 16 in Ireland should not be prevented from such access. Meanwhile Recital 58 makes it clear that children must be given the information and means to understand how and why their personal data is being processed.²⁵ The principle that children should be able to control the use of their personal data is also evident in Recital 65 concerning the right of erasure or "right to be forgotten". That recital contemplates a situation where a child has given his or her consent to the processing of his or her personal data, for example by posting it online, not being fully aware of the risks, and later wants to remove that personal data from the internet.

There tends to be a general misconception that children do not have the same data protection rights as adults, but this is not the case. Children have all of the same rights as adults over their personal data – it is still their personal data and does not belong to anyone else, such as a parent or guardian. As the EDPB's predecessor, the former Article 29 Working Party, stated in its 2009 Opinion on the protection of children's personal data²⁶:

"A child is a human being in the complete sense of the word. For this reason, a child must enjoy all the rights of a person, including the right to the protection of their personal data."

As referred to above, all of the data protection rights which apply to adult data subjects under the GDPR apply also to children. Critically, children do not lose these rights simply because the legal basis relied on to process their personal data is consent and that consent has been given/ authorised by the holder of parental responsibility under Article 8 of the GDPR (i.e. where the child is under the age of consent and the processing concerned relates to an online service²⁷ – see Section 6).

The corollary of the obligations which apply to organisations that process personal data (for example to have a legal basis under Article 6 for processing, or to carry out the

processing in compliance with the principles set out in Article 5) is that data subjects are entitled to have their personal data processed in accordance with all of the rules set out in the GDPR. However, there are a number of specific rights which can be exercised by data subjects directly against the organisation which is processing their personal data, as follows:

- The right to be given certain core information about the processing of the individual's personal data, including who holds it and why it is being processed (**transparency**);
- The right to access and be given a copy of the personal data (**access**);
- The right to rectify inaccurate or incomplete personal data (**rectification**);
- The right to have personal data erased (**erasure – also known as the “right to be forgotten”**);
- The right to obtain the personal data from the data controller and transmit this data to another data controller (**data portability**);
- The right to limit or restrict how the personal data is used (**restriction of processing**);
- The right to object to processing of the personal data (**objection**); and
- The right not to be subject to automated decisions without human involvement (**freedom from automated decision-making**)

It is important to note that these rights are not absolute, and that they are each subject to a number of specific limitations and restrictions. Additionally, certain rights apply to all processing activities, such as the right to information or to access to personal data, whereas other rights only apply in certain circumstances, such as the rights to erasure, restriction, portability, and objection.²⁸ Both the GDPR and the Data Protection Act 2018 set out limitations and restrictions on data protection rights.

2.4 LEGAL BASES FOR PROCESSING CHILDREN'S PERSONAL DATA

Under the GDPR, organisations which process personal data have an obligation to do so lawfully (amongst other things). This means that they must have a legal basis, in other words, a legal justification under the GDPR, for the processing of personal data irrespective of whether it belongs to a child or an adult²⁹.

Article 6 of the GDPR sets out the six possible legal bases for processing personal data. These are either the consent of the data subject or, alternatively, where the processing is necessary for any of the below objectives:

- Performance of a contract or taking steps to enter into a contract
- Compliance with a legal obligation
- Protecting vital interests of a data subject or another person
- Performance of a task carried out in the public interest or through official authority
- Legitimate interests of the data controller or another party (where the interests in question are not outweighed by the data subject's interests or fundamental rights and freedoms).

Data controllers can rely on any of the above-mentioned legal bases for processing a data subject's personal data subject to the circumstances of the processing properly falling within the scope of the relevant legal basis. While there is sometimes a misconception

that consent is the only legal basis for processing personal data, or that it should take precedence over the other legal bases, this is not the case and all legal bases are equal to each other under the GDPR. However, it is important to bear in mind that, as discussed below, certain legal bases require organisations to satisfy additional elements where the data subjects are children, in order to lawfully rely on them.

CONSENT - ARTICLE 6(1)(a)

Under Article 6(1)(a) of the GDPR, processing is lawful (i.e. it has a legal basis) if “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”. Such consent must be **freely given, specific, informed and unambiguous** made by way of a clear statement or affirmative action by the data subject. The consent must also be distinguishable from other matters and **possible to withdraw at any time**. In a real-world, offline context, children can, in theory, subject to having capacity and it being in their best interests to do so themselves (as opposed to by their parent/ guardian), consent to the processing of their own personal data at any age. However, organisations should ensure that where they are relying on the consent of a child to process their personal data, that the child is given a real choice over how their personal data is used and that they have the capacity to provide *informed* consent, e.g. to understand exactly what it is they are consenting to. Where practicable, an assessment of capacity in addition to age, provides a good understanding of the likely capacity at which a child may be able to comprehend a demand or situation, or an age where what is being demanded is beyond their capacity.

Data controllers should also take into account any imbalance of power that might be inherent in their relationship with the child, and must consider whether the consent being provided by the child can truly be deemed to be “freely given”.

In an online context, special restrictions apply where organisations which provide “*information society services*” (i.e. providers of online services) are processing personal data. Article 8 (commonly referred to as the “age of digital consent”) in combination with national law (the 2018 Act in Ireland) sets limitations as to the minimum age (currently 16 in Ireland) at which online service providers can rely on a child’s own consent to process their personal data. For more information on the age of digital consent and the restrictions that apply to relying on consent in an online context, please see Section 5.

CONTRACTUAL NECESSITY - ARTICLE 6(1)(b)

Under Article 6(1)(b) of the GDPR, processing is lawful (i.e. it has a legal basis) where the processing “*is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*”. This legal basis therefore applies where there is an actual or intended contractual relationship between the data subject and the organisation. In the context of processing a child’s personal data, organisations must take into account age restrictions and other specific capacity-related rules which may apply under national laws in relation to the capacity to enter into a contract³⁰ and a child’s competence to understand what it is they are agreeing to. In Ireland, the law in relation to contracts with persons under the age of 18 is complex and the general rule is that at common law such a contract is voidable subject to certain exceptions³¹ (e.g. the concept of “contracts for necessities”³² and contracts of service which are deemed to be beneficial to the person under age 18³³). Given the complexities, nuances and antiquated nature of elements of this area of Irish contract law, organisations which intend to rely on Article 6(1)(b) as a legal basis should carefully consider whether, in all the circumstances, it is an appropriate legal basis for the processing of children’s personal data.

COMPLIANCE WITH A LEGAL OBLIGATION – ARTICLE 6(1)(c)

Under Article 6(1)(c) of the GDPR, processing is lawful where it *“is necessary for compliance with a legal obligation to which the controller is subject”*. Organisations may rely on Article 6(1)(c) in circumstances where they are obliged to process the personal data in order to comply with an obligation which arises under EU or Irish legislation. In order to rely on this legal basis, an organisation must be able to identify the specific legal obligation and to show how it is necessary for them to process the personal data in question in order to comply with that obligation. While the same threshold for reliance on this legal basis will generally apply irrespective of whether an organisation is processing the personal data of adults or children, there may be specific legal obligations which will require the processing of children’s personal data, for example in a child welfare/ protection/ safeguarding/ reporting context. It is of fundamental importance to emphasise that the data protection rules in the GDPR and the 2018 Act (irrespective of whether children’s or adults’ personal data is at issue in any given situation) are not a barrier to safeguarding, and that it is in the ‘best interests’ of children to be protected from violence, abuse or interference/ control by any party.

VITAL INTEREST – ARTICLE 6(1)(d)

Under Article 6(1)(d) of the GDPR, processing is lawful where it *“is necessary in order to protect the vital interests of the data subject or of another natural person”*. This legal basis will apply where the processing of personal data is needed in order to protect someone’s life or to mitigate against a potential risk/ threat/ harm to, or endangerment of, either the data subject or a third party. Given that the GDPR identifies children as being more vulnerable than adults³⁴, the threshold for satisfying this legal basis will generally be lower where the processing of children’s personal data is concerned because what is considered necessary to protect the vital interests of a child may be different (i.e. subject to a lower threshold) to what is considered necessary to protect the vital interests of an adult.

This legal basis is frequently relied on as the legal basis for processing for the purposes of child protection and child welfare measures. The DPC’s comments above, in the context of Article 6(1)(c) on safeguarding-related measures are equally of relevance in relation to this legal basis. Furthermore, and as a general point of note on this issue, **the DPC’s position is that child protection/ welfare measures should always take precedence over data protection considerations affecting an individual. The GDPR, and data protection in general, should not be used as an excuse, blocker or obstacle to sharing information where doing so is necessary to protect the vital interests of a child or children.**

PERFORMANCE OF AN OFFICIAL OR PUBLIC TASK – ARTICLE 6(1)(e)

Under Article 6(1)(e) of the GDPR, processing is lawful where it *“is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”* This legal basis should be read in conjunction with Section 38 and 39 of the 2018 Act. It will generally be reserved to public sector organisations (or organisations acting on their behalf) or organisations performing a public law or statutory function. In this context, there may be specific functions which are required to be performed by organisations captured by this legal basis which require the processing of children’s personal data e.g. in connection with health, social care or education. As a particular point of note in relation to processing carried out for such official or public tasks, the DPC’s position is that organisations processing personal data under this legal basis should comply with these Fundamentals, save where the public interest and/ or



the best interests of the child require otherwise and the organisation can demonstrate why/ how this is the case.

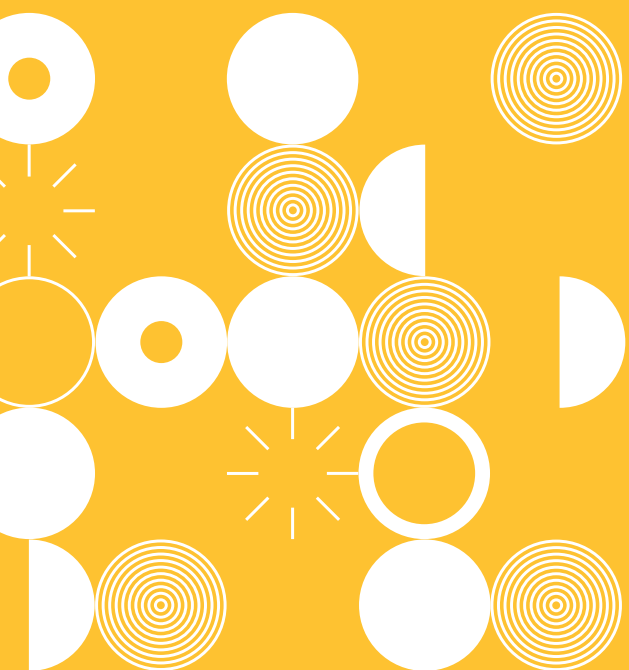
LEGITIMATE INTERESTS – ARTICLE 6(1)(f)

Under Article 6(1)(f) of the GDPR, processing is lawful where it *“is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, **in particular where the data subject is a child**”* [emphasis added]. The central condition for reliance on this legal basis is that the legitimate interests which are pursued by the organisation (or the third party) are not overridden by the interests, rights, and/ or fundamental freedoms of the data subject. This means that the organisation needs to carry out a balancing exercise when assessing whether the processing of children’s personal data should take place. Such a balancing test involves (1) identifying the legitimate interests of the controller or another person/ organisation which are sought to be achieved, (2) demonstrating why/ how processing is a **necessary** and **proportionate** means to achieving the legitimate interests, and (3) balancing those legitimate interests against the child’s interests or fundamental rights and freedoms.

The DPC considers, in light of the principle in international and EU law discussed in Section 2.2, that the best interests of the child should be paramount in any decision-making concerning the processing of children’s data, whether it is undertaken by a private sector or public sector organisation. 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. **This means that organisations processing children’s data in reliance on this legal basis should ensure that legitimate interests pursued do not interfere with, conflict with or negatively impact, at any level, the best interests of the child**. In circumstances where there is any level of interference with the best interests of the child, this legal basis will not be available for the processing of children’s personal data. In practical terms, this means that organisations must carefully examine all of their processing operations on a case-by-case basis with regard to these conditions.

As will be seen from Section 6, the DPC considers that there are certain types of data processing operations consisting of profiling and targeted/ behavioural advertising activities which (subject to certain limited exceptions) will generally not satisfy this principle of **zero interference with the best interests** of a child.





Transparency and children



The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by an organisation and that **this information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The clarity of this information is particularly required where it is being provided to a child.** The essence of the transparency obligation is set out in Article 12 of the GDPR:

Article 12: The controller shall take appropriate measures to provide any information referred to in Article 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

The transparency information that must be provided where an organisation is processing an individual's personal data is set out in Article 13 (which applies where the personal data has been collected directly from the individual) and Article 14 (which applies where the personal data has been collected from a source other than the individual). The information that must be provided by the organisation under these provisions includes: the identity and contact details of the organisation that is collecting or using the personal data; the purposes and legal basis for collecting or using the personal data; who the personal data is being shared with; how long it will be kept for; and what the individual's data protection rights are.

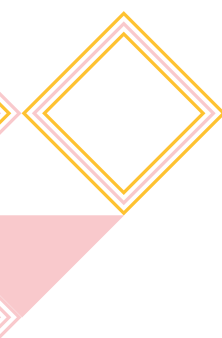
The EDPB has emphasised the importance of transparency as a freestanding right for children³⁵. **This means that children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on e.g. even where a parent or guardian has consented on their behalf to the processing of their personal data.** As referred to above, Article 12 makes it clear that the requirement for clear and plain language is of particular importance when providing information to children³⁶; this is also reflected in Recital 58, which underscores the importance of information being given to children about the use of their personal data in a way that they can easily understand³⁷. As well as considering the age appropriateness of the language itself, children may require information in different formats and at different times in the user journey in order to fulfil this requirement.

Recital 58: [...] Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

3.1 KNOWING YOUR AUDIENCE

It is vital that organisations know who their audiences are (i.e. their customers, users, readers, or visitors to their website or app, or users of their internet of things device, whose personal data they are collecting and using) **so that they can tailor their transparency information for optimum accessibility and understandability.** That being said, the transparency obligation applies just as much in the case of adult data subjects as it does to child data subjects, so complex, legalistic, vague or jargon-driven approaches to providing transparency for data subjects will not suffice in any scenario.

The DPC is not proposing that organisations must necessarily provide two separate sets of transparency information for adults and children where they have a mixed audience of child and adult users. In fact, if the information is clear and simple enough for a child to understand, then it will also comply with the transparency requirement in relation to



adult data subjects. However, where organisations fall within the scope of application of these Fundamentals (see Section 1.3), organisations must assess how to ensure meaningful transparency for child users, according to the age ranges of child users. That may mean implementing child-specific measures which vary according to the audience age ranges of child users or alternatively ensuring that, in the case of mixed audiences where the organisation decides to provide only one set of transparency information, the timing for delivery of this information is meaningful and the mode(s) of delivery and content are clear and simple enough for children of different age groups to easily access and understand.

According to the EDPB, organisations, as data controllers, must ensure that the *“vocabulary, tone and style of the language used [to convey the transparency information] is appropriate to and resonates with children so that the child addressee of the information recognises that the message/information is being directed at them”*.

3.2 METHODS TO CONVEY TRANSPARENCY INFORMATION TO CHILDREN

Article 12(1) requires that organisations take “appropriate measures” to convey transparency information to data subjects, which means that such measures will vary, amongst other things, according to the service being offered. In other words, there is no one-size-fits-all solution for conveying transparency information to children. However, at a minimum, there are a number of basic factors that organisations should take into consideration when identifying appropriate transparency measures for children, such as the device used to access the service (e.g. smartphone, computer, connected devices or toys), whether non-textual methods of communication, such as cartoons and videos, might be more suitable than solely textual methods, or whether electronic means such as layered information notices, hover-over notices or pop-up notices are appropriate³⁸.

USE CLEAR, SIMPLE LANGUAGE

Organisations should use clear, concise and child-friendly language to explain to children exactly what it is that they are doing with their personal data. Children are often unaware that personal data includes things like photos or videos of them, or that their personal data is being collected for specific reasons, such as providing customised in-app experiences, advertisements, or even that their personal data will be retained for a certain period of time³⁹. For this reason, the information set out in Articles 13 (and 14 where applicable) which is required to be delivered, should be in plain, simple language, tailored to the relevant age ranges of the audience. Organisations should be open and honest about exactly what it is they are doing with children’s personal data indicating all of the different ways in which it will be used. This information should also be available in an obvious, easy-to-find place, e.g. not in tiny writing at the bottom of a webpage or app screen. As detailed further in Section 7, information should not appear in a way that nudges the user to accept, for example by appearing as a pop up or making the option to consent more obvious or less obstructive to the user experience than the option to find out more or withhold consent. Children should not have to go searching for this information. These recommendations reflect some of the feedback the DPC received directly from children in its 2019 consultation and examples of these types of comments are set out on the next page.

CONSIDER USING NON-TEXTUAL MEASURES

Organisations should consider using non-textual measures, such as cartoons, videos, images, icons, or gamification, depending on the age ranges of their users, to convey data protection information to children and young people more effectively, as these methods are more likely to resonate with children than blocks of text.

Careful consideration should be given to what methods are more likely to appeal to children using a particular service, according to age and developmental stages. Organisations are encouraged to use formats that are the most applicable/ relevant to the service they offer – for example, if they operate a video-sharing platform, then videos are likely to be a more appropriate means for conveying transparency information to children than an image or a piece of text. If a decision is taken to use written communications to convey transparency information to children, it should be presented in an eye-catching manner through the use, for example, of large font sizes, easy-to-read bulleted lists, bright colours, etc. and it should be presented in “bite-sized” chunks. Children should be presented with the core data protection information up front and should be actively encouraged by organisations to find out more about how their own personal data will be used and how that use will affect them, for example by means of click-through buttons.

WHAT CHILDREN HAD TO SAY ABOUT TRANSPARENCY MEASURES...

"Tell us immediately on signing up for an app how our data will be used before we sign up and agree to the terms and conditions. We would like the chance to think about it first"
(Age 10-11)

"It should be possible to ask someone online questions if you don't understand something."
(Age 12-13)

"Make a cool video or YouTube clip that's fun (and put a timer on terms and conditions to ensure that you read them)."
(Age 12-13)

"Break the information down into bullet points."
(Age 15-16)

"Send us examples of how personal data has been used in the past."
(Age 10-11)

"Make the font larger, more colourful."
(Age 16-17)



"When you input your personal data, they should ask 'Do you want to know where your information goes?'"
(Mixed group, age 8-12)

"Use language children and teenagers can understand easily so that they are properly informed."
(Age 12-13)

The DPC considers that, in addition to data protection by design and default (see Section 7.2), organisations should actively promote privacy-protective measures amongst children by encouraging them to be curious and cautious about the use of their personal data. Children should be empowered to make informed decisions about what personal data they choose to share with an organisation or indeed with a wider audience when using an organisation's service, recommending that they seek parental/ trusted adult support or advice where they are unsure about such choices.

PROVIDE TRANSPARENCY INFORMATION THROUGHOUT THE USER EXPERIENCE

Transparency information should not only be provided just upon sign-up to a service or at the initial point of collection of personal data. Organisations should consider using methods such as just-in-time notifications to inform children and young people about any possible risks or consequences involved in sharing their personal data at a particular moment in time, for example just before they post or share something online or before they change default privacy settings (see Section 7). As referred to above, organisations should also encourage children (through pop-ups or prompts, for example) to ask their parents/ trusted adult if they have any questions about the transparency information they have been presented with.

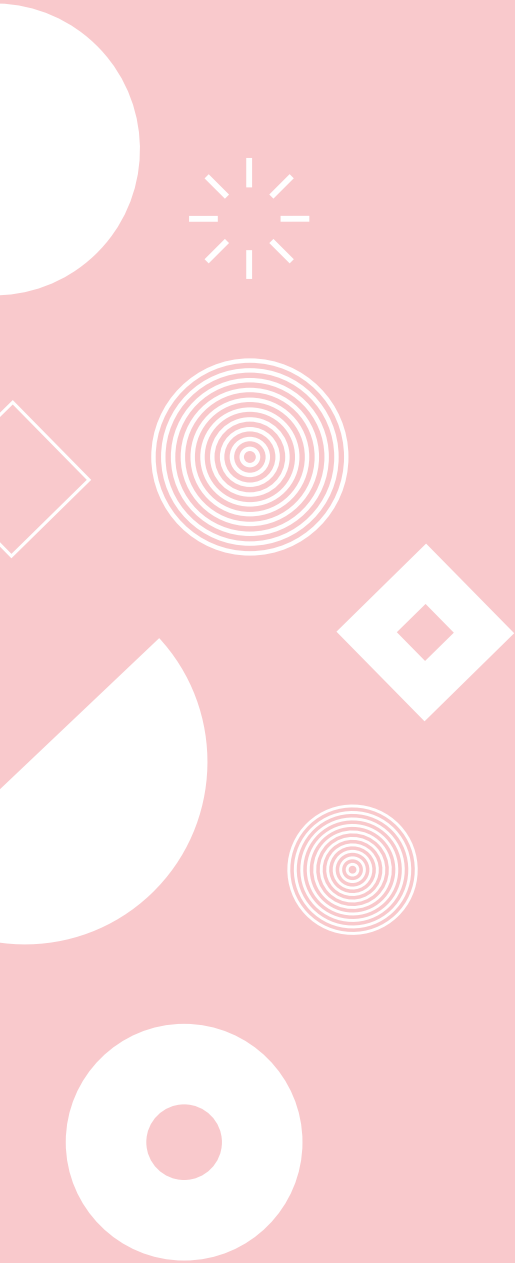
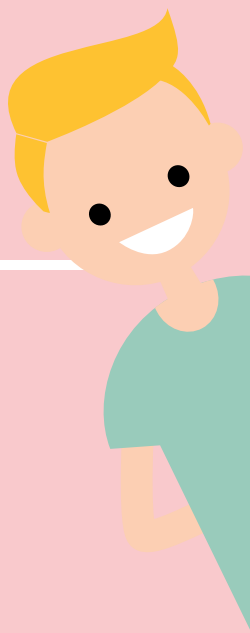
BE EASY TO CONTACT

The DPC also advocates an approach whereby children and young people are given the opportunity to ask organisations who process their personal data questions directly (for example, via instant chat, a dedicated email address, or a privacy dashboard) if they are unsure about any of the transparency information they have received. This contact information for the organisation should be easily accessible to children – they should not have to go looking for it. Additionally, children should be able to expect that response times and customer service commitments in this regard, as outlined in published terms, are consistently upheld.

PROVIDE CLEAR EXPLANATIONS OF USER CONTROL CHOICES AND DEFAULT SETTINGS

As detailed in Section 7, 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. This means that certain types of processing which may pose particular risks to children over and above adult users (for example suggestions of third party contacts who are not existing members of a child's network) must not be provided to children. As part of compliance with its transparency obligations, therefore, an organisation should provide explanations to children as to why certain settings are automatically switched to off or denied to them by default. Warning boxes should appear if the child users try to turn on such settings and information provided explaining why certain user control settings apply to them.

Exercising children's data protection rights



WHAT CHILDREN HAD TO SAY ABOUT THE AGE AT WHICH THEY CAN ASK A COMPANY FOR A COPY OF/TWO ERASE THEIR PERSONAL DATA...

"It would be more helpful to set an age up to which parents could help kids to get their data or delete data."
(Age 8-9)

"As you get older you should be allowed more privacy and to become more independent."
(Age 11-12)

"Any age. You have a right to access your own data. An age should not be required."
(Age 12-15)

"We should be in charge of our personal data but our parents should be allowed access it so we don't get into trouble."
(Age 10-11)

"Any age as you should always have a right to know what companies know about you."
(Age 10-11)

"There should not be an age limit. If you have the capacity to contact them, you are mature enough to do this."
(Youth Group, mixed ages)

"We think you should be 13. A majority of apps require you to be 13 so you can request it then."
(Age 13-14)



Although the GDPR shines the spotlight on the position of children as data subjects in their own right, one issue it does not address is when children should be able to exercise these rights for themselves. The GDPR does not say when, or in which circumstances, a child can make, for example, an access request for, or erasure request concerning their personal data. Nor is there any guidance as to when, or in what circumstances, a parent/ guardian can exercise these rights on their child's behalf. In Ireland, for data protection purposes, a child is somebody under the age 18⁴⁰, which is in keeping with the definition of a child under the UNCRC as "a person under the age of 18 years".

4.1 THE POSITION OF CHILDREN AS RIGHTS HOLDERS

While there is no national law in Ireland which specifies the age at which children have a legal right to exercise their rights as a data subject, it is useful to consider the position in other countries. In Scotland, there is a rebuttable presumption that a child of 12 or over is of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. While this principle does not apply in the rest of the UK, the Information Commissioner's Office (ICO) takes the position that this approach will be considered reasonable in many cases and that a child may exercise their data protection rights on their own behalf as long as they are competent to do so. However a child should not be considered to be competent if it is evident that he or she is acting against their own best interests⁴¹.

In its consultation process with children, the DPC sought and received feedback from children about when they felt they should be able to exercise their own data protection rights (see comments on the previous page). While there appeared to be a general trend in responses of younger children towards having their parents involved in helping them to manage their personal data until they turned 18, the older the age of respondents, the more they moved away from this view and towards a greater insistence on managing their own personal data⁴². However, based on our consultation feedback from adult experts in this area, it would appear that age alone is a far from a perfect metric for assessing the capacity of a child to exercise his or her data protection rights, given that there can be considerable variation in the cognitive development in children of the same age, particularly in early adolescence. Children of different ages have different levels of understanding and needs, and there is no "magic age" at which a new level of understanding is reached. The DPC also notes that the UN Committee in its General Comment on the right of the child to be heard⁴³ 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. Significantly, the UN Committee emphasises that the right to be heard as protected by Article 12 UNCRC (see Section 2.1) 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. Noting this position in international law, the DPC recognises that the exercise of rights by an individual is very closely connected to the right to be heard and indeed can be seen as an expression of the individual's views.

Accordingly, the DPC does not consider that it is appropriate to set a general age threshold as the point at which children should be able to exercise their rights on their own behalf. That being said, while age alone is not the most appropriate benchmark, it should certainly be taken into consideration in conjunction with a number of other

criteria. Therefore, the DPC considers that all of the following (non-exhaustive list of) factors should be taken into consideration in the assessment of whether a child should be capable of exercising their own data protection rights:

- The age and maturity (for example as demonstrated by interactions between the child and the organisation in question) of the child;
- The type of request (access request, erasure request, right to object, etc.);
- The context for the processing and the type of service offered by the controller (e.g. social media platform, doctor-patient relationship, online shopping platform, etc.);
- The type of personal data at issue (e.g. child seeking access to medical data, child seeking erasure of photos of themselves on social media, child seeking to update their email address on a platform). The DPC considers that in cases where the exercise of a child's data protection rights involves access to special category personal data, particularly such as medical data, or access to other sensitive types of data, such as social work data, that careful consideration should be given to whether the release of such personal data could cause serious physical or mental harm to the child in question⁴⁴; and
- Whether enabling the child to exercise their data protection rights themselves is in the best interest of the child (i.e. do they understand the consequences of erasing certain types of personal data, will they fully comprehend what it is they are receiving as part of an access request, will receiving certain information be detrimental to their well-being?)
- Whether the child is seeking to exercise their rights with the assistance/ participation/ knowledge of a parent/ guardian or expert third party/ advocate.

However, even where an organisation decides that it will not facilitate a child to exercise their data subject rights in relation to the personal data which it holds about that child - because it has carried out an assessment and concluded that to do so would not be in the best interests of the child - this should not be the end of the matter. As referred to above, children are still data subjects irrespective of their age and should be facilitated insofar as possible to benefit from the protections for data subjects under the GDPR. This means that an organisation should explain to the child, in a transparent and easy to understand manner, why they have decided not to comply with the request. The child should also be informed that even though the request has not been complied with, they can ask their parent/ guardian or expert third party/ advocate to make the request on their behalf to the organisation.

In sum, **a child may exercise their own data protection rights at any time, as long as they have the capacity to do so and it is in their best interests**. Given the complexity and opaque nature of many

WHAT ADULTS THOUGHT...

When asked at what age children should be able to make access and erasure requests, the most popular answer was "Any age", followed by "16-18" and then "12-15".

Slightly more respondents were in favour of granting erasure requests at any age than access requests, suggesting that respondents had a more paternalistic approach when it comes to access requests but a more enfranchising approach to erasure requests.

Child safety experts argued that age is an imperfect metric for assessing a child's digital maturity, and proposed alternatives such as emotional intelligence, level of education, evidence of extracurricular activities, etc.

Most submissions agreed that parental control over their children's personal data should decrease as they get older, and that children should be in full control of their personal data from the digital age of consent onwards.

Several submissions argued that existing guidance produced by the Office of the Information Commissioner for handling FOI requests could serve as a template for assessing requests by parents to exercise their child's data protection rights.

transactions and interactions which children may have with a variety of organisations, children should also be able to be represented by an adult, either an expert in the field/ advocate or a parent or guardian when exercising their rights or indeed when making a complaint to the DPC.

In all events, **the DPC position is that a child should be able to exercise their data protection rights, whether directly or with assistance/ representation, and should not be prevented from doing so as a result of their age, maturity or capacity.**

4.2 ACTING ON BEHALF OF A CHILD

A child's right to the protection of their privacy is guaranteed by Article 16 of the UNCRC. Meanwhile the rights and responsibilities of parents or legal guardians as protectors and caregivers to ensure the best interests of their children are highlighted under Article 18 of the UNCRC. That being said, Article 5 of the UNCRC recognises that the responsibilities, rights and duties of parents and legal guardians to provide guidance in the exercise of the child's rights under the UNCRC must be consistent with the evolving capacities of the child. As such, the UNCRC recognises that, at a certain point in their development, children will be capable of exercising their own rights on their own behalf.⁴⁵

While there are no specific provisions in Irish law which state that the guardian of a child is entitled to exercise the data protection rights of that child, if a child is under the age of 16, and an online service provider is relying on consent as a legal basis to process a child's personal data, the consent of the child's parent/ guardian is required before the online service provider can process the child's data (see Section 5). Though the provision of consent and access to a child's personal data should be viewed as separate matters, it follows, as considered further below, as a corollary of guardianship status that – insofar as it is in the best interests of the child – that a parent/ guardian of a child should be able to access their personal data.

Parents or legal guardians of a child have a specially protected position under the UNCRC⁴⁶, but their rights and duties must always be governed by the best interests of the child. There is also an obligation on parents or legal guardians to provide guidance to children when it comes to the exercise of their rights under the UNCRC. While the UNCRC does not specifically protect the child's right to data protection, it does, as noted above, protect the child's privacy against arbitrary interference. These are all relevant factors to be taken into account when considering in what circumstances a parent or legal guardian may exercise one or more of their child's data protection rights. In a data protection context, (and taking into account the concept of guardianship under Irish law), this means that the guardian(s) of a child may exercise the data protection rights of his/ her/ their child where it is in the best interests of the child to do so. This in turn must be assessed by reference to a range of factors.⁴⁷

The DPC notes that as a matter of Irish law, there is a rebuttable presumption that a parent/ guardian is acting in the best interests of their child unless there is evidence to the contrary⁴⁸. However, in addition to taking account of this presumption, the DPC considers that the following (non-exhaustive list of) factors⁴⁹ should also be considered by an organisation in deciding whether it is in the best interests of the child that their parent(s)/ legal guardian(s) step into their shoes and exercise their data protection rights:

- The age of the child – the closer the child is to the age of 18, the more likely it is that an organisation holding the child's personal data should deal directly with the child themselves, rather than involving the parent/ guardian. In this regard, the DPC considers that where a child has

reached 17 years, given the closeness of this age to the age of majority (and this notably also being the age at which a driving licence can be obtained as well as the minimum age for sexual consent), other than in exceptional circumstances (i.e. where the best interests of the child demonstrably require it), the child's data protection rights should not be exercised by the parent(s)/ guardian(s). Instead the organisation should deal directly with the child;

- The nature of the personal data and the processing being carried out – this should include consideration of the sensitivity/ confidentiality of the personal data and the basis upon which it has been provided by or shared by the child with the organisation which holds it – for example is there a duty of confidence owed to the child?;
- The nature of the relationship between the child and the parent/ guardian – e.g. are there any court orders relating to parental access/ responsibility/ custody/ child protection etc. in existence?;
- The purpose for which the parent(s)/ guardian(s) seek(s) to exercise the child's data protection rights – for example is this purpose wholly in the best interests of the child or is there another purpose or interest (i.e. that of the parent/ guardian or a third party, as opposed to the child) pursued in seeking to exercise these rights?;
- Whether the child would, or does in fact, consent to the parent(s)/ guardian(s) exercising their data protection rights and any views or opinions expressed by the child;
- Whether allowing the parent(s)/ guardian(s) to exercise the child's data protection rights would cause harm/ distress to the child in any way; and
- Whether there are any sectoral rules or laws which apply to the particular context in which the parent(s)/ guardian(s) is/ are seeking to exercise the child's data protection rights. In this regard, in an educational context, the DPC notes that Section 9(g) of the Education Act 1998 states that a school shall ensure that parent(s) (or in the case of a student who is 18 years, the student themselves) shall have access to records kept by the school regarding the student's educational progress. This creates a statutory right of parent(s)/ guardian(s) of a student to access school records where the student in question is under 18 years. (As an aside, the DPC considers that in complying with this obligation a school may give a choice to a student on reaching the age of 18 as to whether he/ she wishes to directly receive updates on his/ her progress or whether he/ she consents to have his/ her parents continue to receive updates for as long as he/ she remains a student at that school.)

WHAT CHILDREN HAD TO SAY ABOUT THEIR PARENTS EXERCISING THEIR DATA PROTECTION RIGHTS ON THEIR BEHALF...

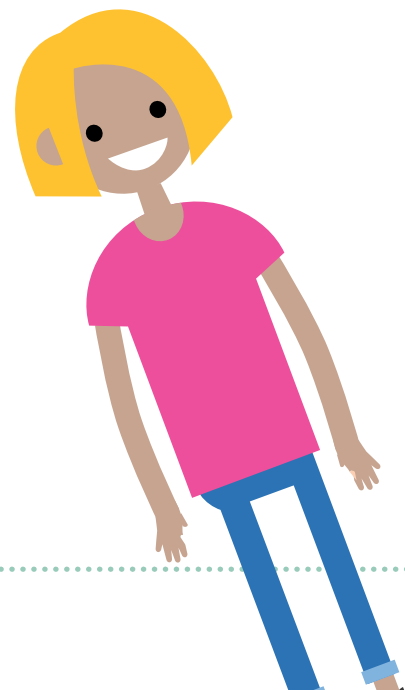
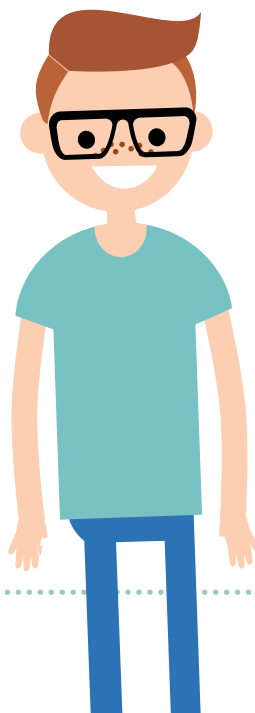
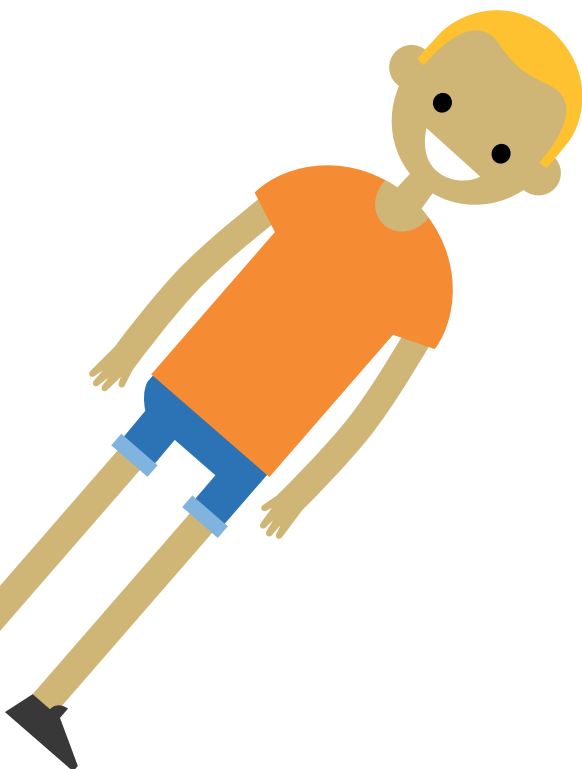
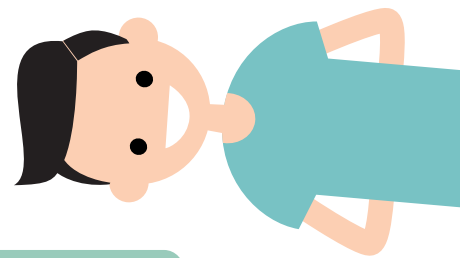
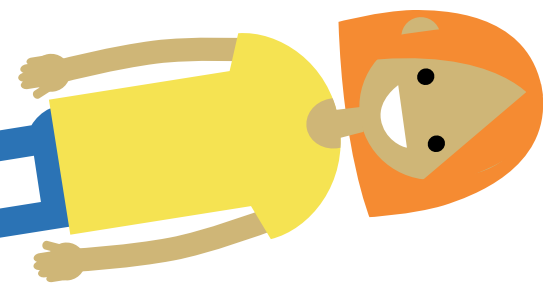
Only 7% of children thought that parents should be involved until they reached the age of 13, while 19% felt their parents should have a role to play until they reached the age of 16.

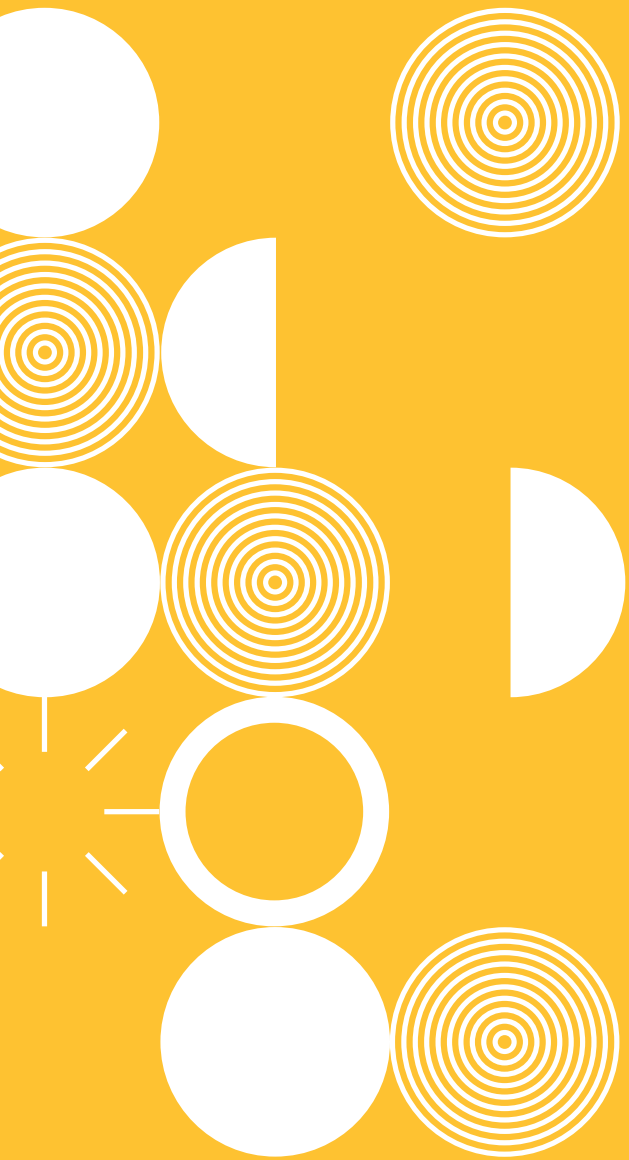
30% of children felt that parents should have no say at all. This option was particularly popular with secondary school students, who accounted for 60% of the 30%.

Approximately 45% of children felt parents should have a role in helping children to manage their personal data until they turn 18. Of these, the vast majority (just under 90%) were students in primary school or in the first three years of secondary school, so roughly 7-15 years.

"It's your business so no parents involved."
(Age 12-13)

"Parents need to know what children are doing online so that they can help keep them safe e.g. giving your number to strangers online, posting photos of yourself in your school uniform."
(Age 8-9)





Age of digital consent and age verification

5.1 AGE OF DIGITAL CONSENT

The concept of the so-called “age of digital consent” in relation to information society services stems from Article 8 of the GDPR which states that if an information society service⁵⁰ (such as a website or an app that offers a service, e.g. gaming, social media, video-sharing, etc.) is being offered directly to a child, and that service is relying on consent as the legal basis to process the child user’s personal data, then parental consent (described in the GDPR as consent from the holder of parental responsibility) must be obtained, in Ireland, if the child is under 16 years of age.⁵¹

If consent to process personal data is requested by the online service provider in order for the child to access the service (for example in the creation and subsequent use of a user account), parental consent must be given for that processing of the child’s personal data to take place. This starting point is that consent must be given by the person who holds parental responsibility, in other words the parent/ guardian of the child. However, as regards the degree of certainty to be established by online service providers that consent has been given by the holder of parental responsibility, the GDPR requires that the online service provider must make “reasonable efforts” to verify this “taking into consideration available technology”.

Of critical importance is the fact that **the requirements around the age of digital consent do not impose restrictions on a child being able to access a service.** Rather the age of digital consent sets the threshold for the age at which a child can give their own consent to online service providers to process their personal data. However, as discussed above, organisations processing children’s data can potentially rely on one of the other five legal bases under the GDPR, instead of relying on consent, to do so. In other words, under the GDPR, consent is not the only legal basis for processing the personal data of children.

It is important to emphasise that the age of digital consent is therefore not a measure to *prevent* access by children to certain websites and apps etc., nor is it an online safety measure; instead it is a measure to *protect the personal data* of children in certain instances. The age of digital consent is also a marker for online services to consider the nature and design of their services, and how to make them age appropriate for their users. **Digital consent obtained from children over the age of digital consent (i.e. 16 or over in Ireland), or from the guardians/parents of children under the age of digital consent, should not be used as a route to treat children of all ages as if they were adults.** As discussed above in Section 2.4, consent must be freely given, specific, informed and unambiguous, and children/ parents or guardians should be provided with easy-to-use mechanisms so that they may withdraw consent at any time.⁵² Collecting consent in accordance with Article 8 is also an opportunity for the online service to provide an age-appropriate data protection regime – by default – adapted to the age ranges of users.

5.2 VERIFICATION OF PARENTAL CONSENT

Age verification for the purposes of ensuring an organisation applies the highest standards of data protection to child users is *different in purpose* from age verification where an organisation relies on consent as the legal basis to process children’s personal data, although the same age verification methods may be used in both instances. (Other purposes for which age verification may be used by an online organisation are considered below in Section 5.3). In the former, age verification is to establish whether a user is under the age of 18 and therefore a child for the purposes of Irish and EU law, thus meriting the special protection identified in the GDPR. On the other hand, age verification for legal basis purposes will generally be aimed at establishing (in Ireland at least), whether a user is under the age of digital consent of 16 years. Notably the GDPR does not require that organisations carry out age verification in order to comply

with Article 8 GDPR. However, it does require that organisations make “reasonable efforts” to verify – where a child is below the age of 16 (in Ireland) – that consent is given/ authorised by the holder of parental responsibility over the child. There are no specified or suggested methods for complying with this obligation and the GDPR simply requires that there must be consideration taken of the “available technology”. This means that organisations must fully explore all of the technological options available to them – and maximise innovation. Given the scale of technical specialities and resources available to technology and internet companies (i.e. whose business models are predicated on deployment of digital and online technologies) and the higher risks to the data protection rights of users who utilise their services, especially children, **the DPC considers that a higher burden applies to such organisations in their efforts to both verify age (see below) and verify that consent has been given by the parent/ guardian of the child user.**

It is however important that the methods employed to verify that consent has been obtained from the actual holder of parental consent are not overly intrusive and that they adhere to the principles of data protection. As with age verification for the purposes of establishing whether a user is a child (see Section 5.3), the DPC considers that a proportionate and risk-based approach should be adopted. This entails a requirement for greater stringency/ levels of certainty provided by the particular verification process where the processing of personal data undertaken by the organisation poses higher risks to the user based on the criteria identified in Section 5.7 below.

This is in line with the EDPB position that recommends a proportionate approach for verifying parental consent that could include obtaining a limited amount of data from parents where necessary (e.g. contact details) in low-risk situations. The EDPB states that whereas low-risk processing by an organisation may only require verification consisting of sending a parent a confirmation email (i.e. to which they must respond), higher-risk processing might call for more thorough verification methods such as requesting proof of ID or requesting payment of a token sum of money by bank transfer. The EDPB suggests that trusted third-party verification services might be an answer to the question of how to verify parental consent without collecting excessive personal data⁵³.

While these represent some of the types of methods which may be deployed to verify the provision of parental consent, the DPC considers that methods endorsed by equivalent regulators in other jurisdictions could also act as a blueprint for the types of methods which may equally be deployed for GDPR compliance purposes. In the USA, the Federal Trade Commission (FTC)⁵⁴ has endorsed the following methods for complying with similar obligations⁵⁵:

1. signing a consent form and sending it to the organisation via fax, mail, or electronic scan;
2. using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
3. calling a toll-free number staffed by trained personnel;

WHAT ADULTS THOUGHT...

Several respondents said that it would be difficult to verify parental consent in a way that respected the principle of data minimisation.

Certain responses referred to neutral age gates used in conjunction with a second validation methodology while others emphasised that age gates should be designed to avoid “back buttoning” and re-entry of dates of birth

A proportionate, risk based approach was suggested by a number of submissions, whereby methods such as email/text verification would suffice for low-risk processing but proof of ID, for example, might be required for high-risk processing.

Several suggested adopting the methods approved by the FTC under COPPA

One organisation suggested using deterrents such as pop-up messages that appear before the parent gives consent, with warnings about fines or being blocked or blacklisted from the site if they fraudulently claim to be the holder of parental responsibility for the child.

Another suggested requesting the electronic signatures of parents to discourage potential bad actors.

Some submissions pointed to the fact that this is a complex legal area from the perspective of guardianship, and that legal provisions around the exercise of parental responsibility vary across EU Member States, making it very difficult to implement a single solution.

4. connecting to trained personnel via a video conference;
5. providing a copy of a form of government issued ID which the organisation checks against a database, which is then deleted upon conclusion of the verification process;
6. answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or
7. verifying a picture of a driver's license or other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.⁵⁶

It is ultimately up to organisations (as controllers) themselves to decide what verification methods are most appropriate and proportionate to the processing which they are carrying out. This should be a dynamic issue which is kept under constant review in light of emerging technologies and which is subject to regular efficacy assessment e.g. by way of user testing and expert involvement.

The “reasonable efforts” that organisations must take to verify the giving of parental consent will very much depend on the nature of the processing of the children's personal data in question and the risks associated with it for the child. This means that there is no standard benchmark as to what constitutes “reasonable efforts” and what might be considered a “reasonable effort” for one online service provider may not be reasonable for another. As noted above, the DPC considers that a higher burden in this regard applies to technology and internet companies (i.e. whose business models are predicated on deployment of digital and online technologies) in light of the higher risks to the data protection rights of users who utilise their services. It is also worth noting in this context that the providers of many online services used by children are also in a commercial relationship with parents and guardians as users in their own rights. Although online services do not currently use these relationships to offer routes to verifying parental consent, it is possible to see how they might do so, potentially limiting the need for additional data collection from the child. In any event, like age verification, all methods of parental verification must be proportionate and privacy preserving, and not involve sharing of a child's personal data.

5.3 AGE VERIFICATION PURPOSES

In order to get to a point where it can verify that a parent/guardian has given consent to the processing of their child's personal data, it may be the case that an online organisation may first have to ascertain whether the user is a child under the age of 16. While the GDPR does not contain an explicit requirement to verify the age of users in order to identify whether or not they are under the age of digital consent, this is the practical implication of Article 8 in most cases⁵⁷. As referred to above, the GDPR does not refer expressly to age verification, and equally it is silent on what might be deemed to be appropriate age verification mechanisms. Consideration of such mechanisms is set out further below.

However, and as referred to above, age verification when undertaken by organisations in support of reliance on consent under Article 8 as the legal basis for the processing of personal data is **just one of the situations in which age verification methods may be employed**. The DPC recognises that there are other purposes for age verification undertaken by an organisation, including:

- allowing access to its service – for example where an organisation provides an adult-only service which by law it cannot provide to under 18s e.g. gambling related services; and
- providing a “child-friendly” version of a service which attracts a mixed user audience i.e. by offering enhanced data protection settings/ features for child users, in line with the requirements of these Fundamentals.

5.4 AGE VERIFICATION AND THE CHILD’S USER EXPERIENCE

Having reviewed the responses to its 2019 consultation, the DPC notes the concern that online age verification measures may be perceived by children as blocking them from the more complete “full” service offering, or as blocking them from accessing other features of the service they are seeking to use⁵⁸. The DPC notes that the likelihood of this perception by child users has also been raised by experts in the fields of child rights, child safety and child advocacy.

While an organisation’s choice as to whom it will offer its services falls outside the scope of the data protection per se, the DPC’s position is that the specific requirements of Article 8 (including the associated implication that age verification underpins verification of parental consent), or any other obligation under the GDPR, including **compliance with the requirements of these Fundamentals, in no way justify the “locking out” of children from a rich user experience simply on the basis of purported data protection compliance**. Similarly, the provision of a two-tier approach with an inferior level of central services and features offered on the one hand to child users while on the other hand, adult users are offered a more superior service, risks depriving children of their full rights under the UNCRC. For example, this risks interfering with the child’s right to express their views fully⁵⁹, their right to freedom of expression and to seek, review and impart information and ideas of all kinds⁶⁰, amongst others. Such an approach, where organisations impose age verification measures in order to filter child users from adult users resulting in a denigration in service levels, also risks driving children “underground”; in other words where they feel compelled to lie about their age in order to access what they perceive to be as a more fulsome “adult” service⁶¹. This in turn can be counter-productive on the organisation’s part in that it may result in child users circumventing age verification measures and accessing a service which does not adhere to the highest levels of data protection, as required under the GDPR for children.

Nonetheless, efforts can be made by online providers to positively support higher standards of protection of children’s personal data with messaging on their service that promotes the advantages to children and parents of these enhanced protections.

The DPC considers that the user experience offered to child users should be adapted in order to minimise, to the greatest extent possible, the risks posed to children from the processing of their personal data in the context of using/ accessing a service, without a deterioration in the overall user experience and the availability of the central features, for which children primarily access the service. High levels of data protection by design and default (see further consideration of this issue in Section 7) also ensure that children are not targeted with age-inappropriate content, such as pornography, which children describe as being a negative experience.⁶²

5.5 MINIMUM USER AGES

The DPC also notes that it is common practice amongst many of the most popular online service providers to apply a minimum user age of 13. However, the DPC does not consider that the setting of a minimum user age obviates the requirement on such service providers to comply with their obligations towards child users below this age, where children are likely to use the service in question. **Where a service provider stipulates that their service is not for the use of children below a certain age, they should take steps to ensure that their age verification mechanisms are effective at preventing children below that age from accessing their service. If the organisation considers that it cannot prevent children below its stipulated age threshold from accessing its service, then the organisation should ensure that appropriate standards of data protection measures are in place to safeguard the position of child users, both below and above the organisation's official user age threshold.** This means that where, in reality, children are able to, or indeed do, circumvent age verification mechanisms and access the service, there is an obligation on the organisation to comply with the controller obligations under the GDPR, and the standards and expectations set out in these Fundamentals, with regard to “underage” users, as well as users who, whilst they may be above the minimum user age, are still under the age of 18. As such, the DPC does not accept that theoretical minimum user age thresholds displace GDPR controller obligations of organisations in relation to “underage” users.

As explained earlier, where an organisation's services are directed at/ intended for, or likely to be accessed by children, irrespective of any age verification measures that an organisation deploys, the organisation should ensure that child-specific data protection measures are in place to enhance the level of protection afforded to child users (irrespective of the official minimum user age) against the risks posed to them by their use of/ access to the service. Further detail on these obligations is set out in Section 7.

5.6 AGE VERIFICATION MECHANISMS

The technological area of age verification mechanisms and tools is still very much in development. As part of its 2019 consultation, the DPC sought input from industry on what it considered to be appropriate methods for age verification. However responses from industry were, overall, rather limited in terms of innovation, with many submissions reluctant to put forward any specific suggestions. Some of the suggestions which were submitted are detailed in the sidebar. Other possibilities for age verification include technical measures such as neutral age gates, use of artificial intelligence methods (e.g. analysing user interactions with a service), as well as self-declarations, official identifiers and existing account information. As discussed further below, the method most appropriate for establishing the age of users will depend on the nature of the online services and the risks posed to children by data processing.

The DPC considers that it is ultimately for industry to continue to innovate in this area. However, any age verification mechanisms

WHAT ADULTS THOUGHT ABOUT AGE VERIFICATION...

Suggestions submitted to the DPC's public consultation included implementing age gates, employing two-step verification methods, requesting official ID, utilising secure third-party verification services, and employing device-level verification methods. Most respondents stated that the most appropriate method will depend on the context and the sensitivity of the data;

Some organisations also suggested that age verification may not be the answer, stating that we need to create an environment in which children feel they can be honest about their age when they sign up for an online service, and that if a child declares themselves to be under 16, then a variety of protections should follow, for example educational popup messages, zero collection of personal data, appropriate filtering, etc.

Another organisation stated that data controllers should not be able to rely on consent as a lawful basis for processing children's personal data if they are not able to clearly demonstrate that they have effective and proportionate age verification measures in place.

developed and utilised must comply with the obligation of data protection by design and default and must also be subjected to data protection impact assessments in order to assess whether the mechanism in question complies with the principles of data protection, including in particular, data minimisation, purpose limitation, storage limitation, and security.

There is unlikely to be a one-size-fits-all solution to the issue of age verification. Appropriate age verification mechanisms are likely to vary from context to context, depending on, for example, factors such as the service being provided and the sensitivity of the personal data being processed. In any event, such measures should be proportionate and grounded on a risk-based approach. This means that there should be greater stringency/ levels of certainty provided by the particular verification process where the processing of personal data undertaken by the organisation is of higher risk to the user based on the criteria identified below in Section 5.7. For example, self-declaration may be suitable for low-risk processing or when used alongside other techniques, while some online services that present a high risk arising from data processing may require more stringent methods of age verification. This could be effected via technical measures which discourage false declarations of age or identify. Finally, it is important to remember that age verification is just one of the two categories of tools that online service providers may use to comply with the Fundamentals. As noted at the outset, the alternative is a “floor of protection” across the service that provides high levels of data protection for adult and child users without distinguishing between the two.

5.7 CRITERIA FOR A RISK-BASED APPROACH TO AGE VERIFICATION

If organisations decide to implement age verification mechanisms, there are certain minimum criteria which should be considered when determining the approach. What may be considered a suitable approach for one organisation may be entirely unsuitable for another. The following list contains a non-exhaustive selection of criteria⁶³ which should be taken into account in adopting a risk-based approach to verification:

- (A) Type of personal data being processed – e.g. health information, images/videos, technical online identifiers, contact details (e.g. full name/age/address/ email address/ phone number), information about religious beliefs or sexual orientation, information about hobbies or interests, etc.
- (B) The sensitivity of said personal data – e.g. special category personal data, or data which could be considered sensitive for other reasons such as financial information, information on family circumstances or birth status or data which also incorporates the data of a third party such as a family member or friend etc.
- (C) Type of service being offered to the child – e.g. video or image hosting platform, educational service, healthcare or social support service, social media app facilitating connections with known parties or with strangers, gaming website, shopping platform, etc.
- (D) The accessibility of the personal data collected to other persons – e.g. whether the nature of the service is to publish or make available the personal data, or elements of it, to the world at large.

-
- (E) The further processing of personal data including whether data collected is shared with other organisations and the reasons for doing so – e.g. for advertising, marketing or profile building purposes by either the organisation or a third party with whom the data is shared.

The most stringent age verification methods will always be necessary for online services where the risks arising from data processing or the activities conducted through such services are illegal for children to participate in, for example, where an organisation provides an adult-only service, such as gambling, which by law it cannot provide to under 18s.





Direct marketing, profiling and advertising



Risks associated with the processing of children's data are amplified by the inclusion of certain design features and marketing techniques, such as profiling and behavioural advertising, or the identification of a child's whereabouts in the processing of geolocation data. The GDPR does not impose an outright prohibition on organisations marketing (i.e. advertising) to children⁶⁴, but it does require that there be specific protections for children when marketing to them or creating user profiles.

Notably, Recital 38 states that the specific protection merited by children *"should, in particular, apply to the use of personal data with regard to children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."* In its 2013 Opinion⁶⁵ on Apps on Smart Devices, the EDPB's predecessor, the Article 29 Working Party, stipulated that, in the best interests of the child, companies *"should not process children's personal data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing"*. The EDPB has reiterated this principle in its guidelines on automated individual decision making and profiling and states that **organisations should, in general, avoid profiling children for marketing purposes**, due to their particular vulnerability and susceptibility to behavioural advertising. This is especially the case for online games and other information society services that use profiling to identify users that can be encouraged to spend more money⁶⁶. The Council of Europe has expressed similar views,⁶⁷ as has the ICO's Age Appropriate Design Code.

6.1 DIRECT MARKETING

Direct marketing usually involves an organisation attempting to promote a product or service.⁶⁸ Where such marketing activities are carried out through the sending of emails, texts, faxes, or telephone calls it is commonly referred to as electronic direct marketing. Electronic direct marketing is governed in the first instance under the ePrivacy Regulations (SI 336/2011)⁶⁹. Regulation 13 of this legislation sets down very strict rules which must be complied with by organisations engaged in the sending of unsolicited electronic direct marketing communications by telephone, SMS, email and fax.

If an organisation engages in the sending of electronic direct marketing, it needs the affirmative consent of the individuals it wishes to send those messages to (such as by specifically opting-in to receive marketing communications) under Regulation 13 of the ePrivacy Regulations⁷⁰. This requirement for consent applies regardless of whether the material is being sent to an adult or to a child.

The consent required to receive such electronic direct marketing communications is the same standard as that set out in the GDPR, in other words it must comply with the requirements of, amongst others, Article 4(11) (definition of consent) and Article 7 (conditions for consent)⁷¹. Even where an organisation undertaking direct marketing has the consent of a person to send them such communications, that consent may be withdrawn. Every electronic direct marketing message sent to a person who has consented to receiving such communications must contain a valid means to allow them to opt out free of charge. It is likely that the age of digital consent, as per Article 8 of the GDPR (see Section 5.1 above), applies to electronic direct marketing communications which are sent by SMS and email⁷² as it would seem that communications sent by these modes fall within the definition of "information society services" as referred to in Article 8 GDPR⁷³. Accordingly, consent to the receipt of electronic direct marketing messages sent by SMS and email can only be provided by a child who is 16 years or over or by a parent/guardian of a child who is under 16 years in line with the provisions of Article 8. Irrespective of the issue of consent, organisations seeking to send such marketing messages to children should take note of the principles set out further below concerning

the best of interests of children in this context.

Aside from where the recipient has consented to receive electronic direct marketing messages, there are certain other circumstances in which organisations can legally send electronic direct marketing messages to individuals⁷⁴. This includes a situation where an organisation obtains a person's details as a result of the sale to them by the organisation of a product or service (i.e. in the context of a customer relationship). Here, the rule is that the person must be clearly and distinctly given the opportunity to *object* to the use of those details for future direct marketing. This is known as a "soft opt-in" rule. The principles concerning transparency for children (set out in Section 3 above) equally apply to the information that must be given to children in this scenario so that they can understand that they have the right to "opt out" of any future marketing messages and so that they can easily exercise this preference. Again, organisations seeking to send marketing messages to children on the basis of the "soft opt-in" rule, should take note of the principles set out further below concerning the best of interests of children in this context.

6.1.1 LEGITIMATE INTERESTS AND DIRECT MARKETING

Businesses may in some cases consider that they have a legitimate interest to engage in direct marketing. It is important to note, however, that while Recital 47 of the GDPR indicates that "*direct marketing may be regarded as carried out for a legitimate interest*", this will in practice only be permitted in limited circumstances. It may apply, for example, to the sending of direct marketing material by post or to marketing material that is served to a wide audience rather than targeted at an individual. Where consent is required for electronic direct marketing under the ePrivacy Regulations, as explained above, an organisation may not seek to substitute another legal basis such as legitimate interests for the requirement to obtain the consent of individuals. This is because the special rules applying to unsolicited electronic direct marketing under the ePrivacy Regulations take precedence and must be applied before the GDPR rules. Therefore legitimate interests cannot be relied on in such a case.

Where any organisation seeks to rely on legitimate interests as a lawful basis for engaging in other (i.e. non-electronic) forms of direct marketing (e.g. by post) the provisions of Article 6(1)(f) of the GDPR apply. Generally speaking, the balancing test required when relying on this legal basis must meet a high threshold to demonstrate that the legitimate interests of the data controller (or third party, where applicable) were not overridden by the interests or fundamental rights or freedoms of individuals. However, as set out in Section 2.4 on legitimate interests, the DPC considers that organisations processing children's data in reliance on this legal basis must ensure that the legitimate interests pursued do not interfere with, conflict with or negatively impact, **at any level**, the best interests of the child. This is discussed in the context of marketing in further detail below.

6.1.2 GDPR RIGHT TO OBJECT TO MARKETING

Article 21: (...) *Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.*

Recital 70: *Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.*

The GDPR provides additional safeguards for individuals in relation to the processing of their personal data for the purposes of direct marketing more generally. Under Article 21(2) of the GDPR an individual has the right to object at any time to the use of their personal data for direct marketing, which includes profiling related to such direct marketing (profiling is discussed further below in Section 6.2). Where an individual exercises this right to object, Article 21(3) provides that their personal data *shall no longer be processed for such purposes*. This right to object must be explicitly brought to the attention of individuals and presented clearly and separately from any other information. In this regard where the personal data of children is being processed for direct marketing purposes, whether the marketing is done through electronic forms or otherwise, (as noted above and below, this must be compliant with the requirements for legal basis and the best interests principle), it should be made clear to children that they may object to the use of their data in this way. Such information should be conveyed in accordance with the principles set out in Section 3 above.

6.1.3 CONSENT FOR MARKETING TO CHILDREN

As noted above, the rules on the age of digital consent are likely to apply to electronic direct marketing messages which are sent by SMS and email which means that only children of 16 or over can consent on their own behalf to receive such messages. With other modes of direct marketing messages, there is no minimum age requirement for a child to consent to the processing of their personal data. *In theory* this means that organisations can conduct some marketing activities towards children where their consent has been obtained. However in any case where an organisation is considering directing marketing activities towards children, it should be extremely cautious about doing so⁷⁵.

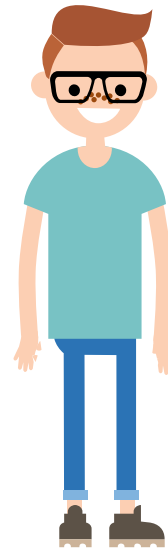
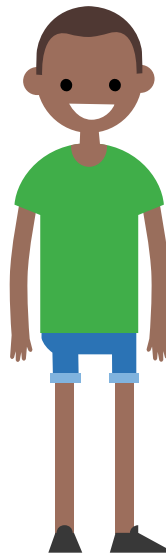
Organisations must ensure firstly that any consent from a child which is relied on is in accordance with the requirements of the GDPR, in other words, freely given, specific, informed and unambiguous. This means that the child who has “opted in” or signed up to receive marketing material should, amongst other things, be fully informed about the use of their personal data. In this regard, the transparency obligations discussed in Section 3 are fully applicable. The child should be able to understand, as a matter of age/ capacity, what the consequences are for them as a result of consenting to the processing of their personal data for marketing purposes.

WHAT CHILDREN HAD TO SAY ABOUT COMPANIES USING THEIR PERSONAL DATA TO SHOW THEM ADS...

60% of children and young people did not think that companies should be allowed to use their personal data to offer them personalised ads, with children aged 10 to 12 the most opposed to this.

Those who were against personalised ads argued that they are annoying, an invasion of privacy or that companies had no business using their personal data for profit.

Other children recalled unsettling experiences of being "followed" by personalised ads on the internet, and one group of 8-9 year olds drew parallels between TV ads and online ads, saying that online ads "are so scary because they are pointed at you directly and not at everyone like a TV ad".

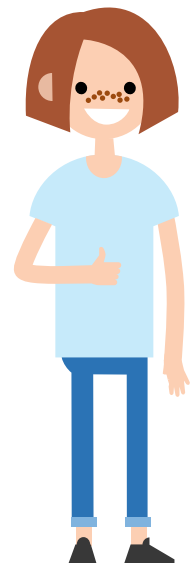


One class was also concerned by the financial pressures that these ads put on parents.



On the other hand, 40% of children and young people thought that companies should be allowed to use their personal data to serve them personalised ads.

Children aged 12-14 were most likely to be in favour. These children often pointed to the convenience of tailored ads. Others were less enthusiastic but accepted that they were necessary in exchange for a free service.



However, critically, organisations must adhere to the principle that, in deciding whether to market to under 18s, the best interests of the child remain paramount. This applies both where consent is relied on (whether given by a child, or a parent/ guardian on their behalf, as applicable) and equally where an organisation relies on one of the other applicable provisions to carry out electronic direct marketing activities, such as the “soft opt-in” rule described above which applies in the context of obtaining a person’s contact details through a customer relationship.⁷⁶ **Should organisations decide to conduct electronic direct marketing activities towards children, they should be able to demonstrate how this is in the best interests of the child, irrespective of any business model or commercial interests of the organisation.** Equally, where non-electronic direct marketing (such as postal marketing) is concerned, while there is no outright prohibition on conducting such activities towards children, the best interests of the child principle remains the key criterion in assessing whether the conduct of such activities is in line with the principles concerning the special protection of children under the GDPR.

As previously noted, Recital 47 of the GDPR provides that processing for direct marketing activities may be regarded as carried out for a legitimate interest. However, as discussed in Section 2.4 this means that organisations processing children’s data in reliance on this legal basis must ensure that the legitimate interests pursued do not interfere with, conflict with or negatively impact, at any level, the best interests of the child. In the context of direct marketing, whether electronic or otherwise, the DPC considers that data processing operations consisting of profiling (see Section 6.2 below), marketing and advertising activities in pursuit of commercial/ business interests of an organisation will generally not align with the DPC’s position that there should be zero interference with the best interests of the child in the processing of their personal data. Therefore unless an organisation can show that the direct marketing activities in question which rely on the processing of children’s personal data to carry out the marketing positively promote the best interests of the child (irrespective of the legal basis being relied on to do so), such activities should not be undertaken. Examples of areas where direct marketing may be used to positively promote the best interests of children include direct marketing of: counselling or support services; educational, health and social services; and advocacy and representative organisations.

6.2 PROFILING AND AUTOMATED DECISION-MAKING

Profiling is a way of using someone’s personal data to predict or analyse characteristics of that person, such as services they will be interested in, their likes or dislikes, preferences, views or opinions, or their behaviour⁷⁷. For example, organisations may collect information from/ about their customers or users to try to predict other services or products they might be interested in.

Profiling can also extend to using the personal data compiled in a profile on an individual to make automated decisions about them (e.g. using algorithms or artificial intelligence where there is no human element involved). Article 22 of the GDPR prohibits automated decision-making about individuals where the decisions made can have legal or similarly significant effects (e.g. relating to, amongst other things, contractual

WHAT ADULTS THOUGHT...

Most submissions argued that where the rights of children clash with the legitimate interests of organisations, the former should always take priority.

Many felt that the legitimate interests of the controller should only apply in a limited set of circumstances. Factors which could be taken into consideration when assessing grey areas including the level of cognitive development of the child, the risk of the processing, the sensitivity of the data, etc.

61% of submissions were in favour of banning the profiling of children for marketing purposes, and 39% were opposed.

Those opposed were primarily technology companies who argued that the GDPR does not explicitly prohibit the profiling of children and that it should be up to parents to decide.

Those in favour emphasised the vulnerability of children and argued that parents often lack the knowledge and expertise to make informed decisions on their children’s digital lives.

or legal rights⁷⁸), unless the organisation carrying out the decision-making can show that one of the exceptions to this principle set out in Article 22(2) applies.⁷⁹ Importantly Recital 71 says that measures relating to “solely automated decision-making, including profiling, with legal or similarly significant effects”, “should not concern a child”. The EDPB has stipulated that **solely automated decision-making, including profiling, which produces legal or similar effects should not be used for children**. Moreover, according to the EDPB, exceptions to the rule against this form of processing should not be relied on in relation to processing children’s data other than limited circumstances such as where it is necessary to protect their welfare.⁸⁰ The EDPB has also recognised that in certain circumstances, targeted advertising based on profiling may fall within the prohibition in Article 22 because it may have significant effects e.g. on vulnerable adults or minority groups. In a similar vein, the EDPB has also recognised that children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising.

6.2.1 USER PROFILES AND TRACKING TECHNOLOGIES

A user profile can be a valuable tool in revenue terms for an organisation because the detailed information on an individual contained in a profile can help the organisation to tailor advertisements and marketing materials, amongst other things, precisely to an individual’s interests, needs or individual views. This is known as “behavioural advertising”, “targeted advertising” or “personalised advertising”. In an online context, profiling of individuals by tracking their online journey across different websites and through the use of different apps on multiple connected devices, and recording their activities and behaviour via such devices and services to glean information about them, has proliferated in recent years.

Such profiling is facilitated by the use of cookies and similar tracking technologies deployed on websites, in apps and even in connected toys. (The DPC has published separate guidance on the use of cookies⁸¹).

The ePrivacy Regulations require that cookies, other than those that are considered ‘strictly necessary’ to deliver the requested service, require the consent of the user. While the cookies themselves may not contain personal data, the use of cookies may result in the processing of personal data either by the organisation directly, or by third parties whose cookies are set on the user’s device. The GDPR explicitly recognises online identifiers (which may include unique identifiers in cookies) as personal data in Article 4(1). The provisions of the ePrivacy Regulations apply to the setting of cookies. However, any processing of personal data that subsequently *results from the use* of cookies is fully subject to the provisions of the GDPR.

Where a product or a service uses cookies, the organisation should conduct audits to establish how these cookies might be used to profile individuals and they should have particular regard for how children may be targeted as a result of their use.

Any user interface seeking consent for the use of cookies (such consent should comply with all the requirements of the GDPR as set out above in Section 2.4) should, especially where the product or service is targeted at children, be easy to understand and it must also provide clear and comprehensible information written in a child-friendly way to explain what cookies do and how the information obtained through the use of cookies will be used, and by what other organisations. Such a user interface which is seeking consent for the use of cookies from children should comply with the transparency principles set out in Section 3. In any event, the use of cookies by organisations should comply with the principles concerning the profiling of children for advertising/ marketing purposes as set out in this Section 6.



WHAT CHILDREN HAD TO SAY ABOUT PERSONALISED ADS...

"Young people use social media as "quiet" time for themselves, so they don't want to be distracted by advertisements."
(Age 12-13)

"It's a bit creepy, if you were just talking about something with your friend and then you get ads about it. It feels like they are listening to you with a secret microphone."
(Age 12-13)

"It feels like they're stalking you."
(Age 8-12)

"There are also really inappropriate ads that pop up and you are not able to skip them."
(Age 9-10)

"It's unfair to target kids with ads to buy things. Kids/families might not be able to afford them."
(Age 11-12)

"[...] we think [ads are] creepy but at the same time we wouldn't pay to join these sites."
(Age 10-11)

"Can be distracting and irritating to see the same ad repeatedly."
(Age 16-17)



6.2.2 ADTECH

The advertising technology industry (known as “adtech”) is a complex ecosystem of many different types of organisations including advertising agencies and networks, data brokers, data analytics companies, publishers and buyers. Those organisations are engaged in high-speed and high-volume digital transactions, selling, sharing, transmitting and aggregating personal data harvested through the use of tracking technologies such as cookies with the aim of serving highly tailored ads to individuals based on what is known or what can be inferred about them. This means numerous organisations can hold many pieces of personal data on one individual. This complicated myriad of invisible activity is difficult for adults to understand let alone for children to comprehend. Academic research has shown that while children easily understand how devices and apps record their data, they have trouble grasping more abstract concepts such as profiling, cross-device identification and metadata to name a few. They are often unaware that many of their favourite platforms are owned by the same company and are often surprised by the amount of information they have to provide in order to access their favourite online services, particularly when this information appears to have little to do with the service being offered.⁸² Equally, children are less likely to be aware that these platforms are free to users because they gather and sell/ share vast amounts of their data – including automatically derived metadata such as time stamps (as to when sites or apps were visited or interactions conducted on them) and location data – to data brokers and data analytics companies who can use it to target them with personalised ads.⁸³ Children’s limited understanding of how their personal data is processed and for what purposes in these complex types of ecosystems further underscores the importance of transparency information being specially tailored to children as outlined in Section 3 above.

6.2.3 CAN ORGANISATIONS USE CHILDREN’S PERSONAL DATA TO PROFILE THEM AND MAKE AUTOMATED DECISIONS ABOUT THEM?

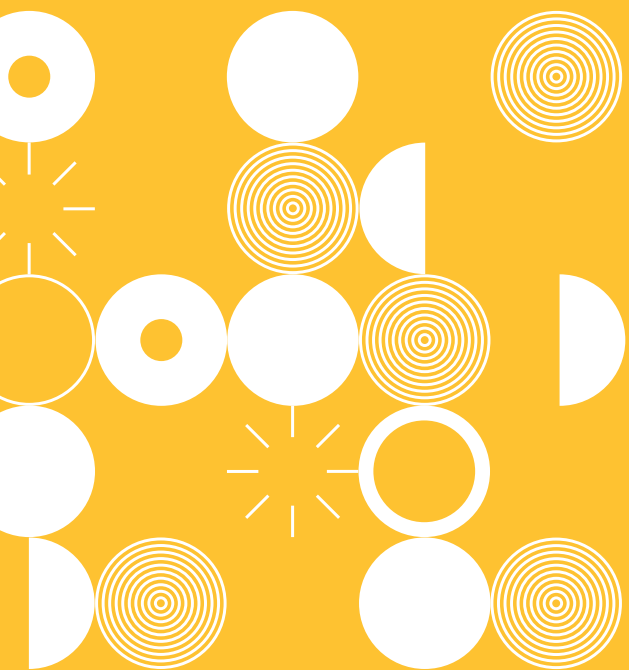
It is the DPC’s position that **organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.** For the avoidance of doubt, the DPC does not consider that it is in the best interests of children to show them advertisements or auto-suggestions for other games/ services/ products/ videos etc. which they might be interested in where such advertisements or suggestions are based on profiling.⁸⁴ Accordingly there is a high burden of proof on the organisation to show how it is in the best interests of children to process their personal data for the purposes of profiling and/or automated decision making, or otherwise, in order to advertise/ market/ make auto-suggestions to them⁸⁵.

The DPC therefore considers that there will be a very limited range of circumstances where the profiling of children and/or the use of automated decision-making concerning children are legitimate and lawful activities under the GDPR. Such exceptions to this may include, for example, the pursuit of these measures to protect children’s welfare⁸⁶.

In any event, if an organisation decides to profile, and/or engage in automated decision-making about, children for any purpose, they must first carry out a data protection impact assessment (DPIA) to establish whether their processing will result in a high risk to the rights and freedoms of children. The best interests of the child must be a critically considered factor in the carrying out of a DPIA concerning the processing of children’s personal data (further information on DPIAs can be found below in Section 7). If an organisation decides that it is actually in the best interests of children to profile them and/or engage in automated decision-making about them for a particular purpose,

that organisation must be able to demonstrate that it has appropriate safeguards in place to protect children. It must also explain to children, in language which they will understand, what personal data is being used in this way, why this is being done and what the real-life consequences are for the child user in doing this.





Tools to
ensure a high
level of data
protection for
children

Article 24(1): *“Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”*

The obligation on organisations, as data controllers, to ensure that children have the benefit of “specific protection” under the GDPR derives in part from Article 24 which requires that controllers must take into account the risks of varying likelihood and severity for the rights and freedoms of natural persons and implement appropriate technical and organisational measures to ensure that processing complies with the GDPR. Given that the GDPR identifies children as vulnerable natural persons and calls out specific protections for children in a number of different contexts, organisations must ensure that they take special account of the position of children as data subjects and implement child-oriented measures to safeguard children against the risks posed by the processing of their personal data. This is particularly so in the context of the data controller obligation to conduct data protection impact assessments and in the context of the principle of data protection by design and default.

7.1 DATA PROTECTION IMPACT ASSESSMENTS

Article 35: *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

Article 35 GDPR states that a Data Protection Impact Assessment (“DPIA”) must be conducted by a controller where a type of data processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. The GDPR also sets out a number of specific instances in which controllers must conduct a DPIA. A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. If required, a DPIA must be completed prior to the commencement of the relevant data processing. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

The GDPR does not explicitly consider the processing of personal data of children to be a processing activity that carries a *high* risk, but the EDPB’s Guidelines on Data Protection Impact Assessments⁸⁷ list “*vulnerable data subjects*” (to include children) as one of the criteria that could trigger the need for a DPIA⁸⁸. Additionally, under Article 35(4) of the GDPR, supervisory authorities like the DPC must establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA. In its published list, the DPC has identified that a DPIA will be mandatory for processing operations involving “*profiling vulnerable persons including children to target marketing or online services at such persons*”⁸⁹. A large number of other EEA data protection authorities have included processing operations involving children in their published lists of processing operations which require a DPIA.⁹⁰

The DPC considers that the principle of the best interests of the child, discussed earlier, requires that **organisations whose services are directed at/ intended for children, or likely to be accessed by children, should carry out a DPIA in respect of the different types of processing operations which are carried out on the personal data of child users.**⁹¹ Such risk assessments should take account of varying ages, capacities and developmental needs of child users as well as considering both actual and potential risks arising from data processing to the health, well-being and general best interests of the child, including social, mental, physical and financial harm. The best interests of the child principle must be one of the primary risk evaluation tools when carrying out a DPIA concerning the processing of children's personal data.

The DPC considers that where organisations have conducted (or have failed to do conduct) a thorough and meaningful DPIA in relation to the processing of personal data of child users, this will be a relevant factor in any assessment by the DPC of an organisation's compliance with its obligations under the GDPR, particularly in relation to the controller's responsibilities under Article 24 including the obligation to take account of the varying likelihood and severity of risks posed to individuals as result of the processing of their personal data. A child-oriented DPIA is the first step in mitigating risk arising from processing children's personal data, and will be seen as a key act of compliance with existing legal requirements for protecting the position of children as data subjects.

7.2 DATA PROTECTION BY DESIGN AND DEFAULT

Article 25 states that controllers must "[...] implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

The GDPR imposes a new obligation of data protection by design and by default on organisations which process personal data. Article 25(2) of the GDPR emphasises the requirement for default technical and organisational measures concerning data minimisation, purpose limitation and data retention.⁹² This means that **data protection measures should be built into the architecture and functioning of a product or service from the very start of the design process (rather than being considered after the development phase) and that the strictest privacy settings should automatically apply to a product or service.** The user should not have to deactivate (e.g. switch to off) settings which interfere with a person's privacy such as location tracking, health settings which track the movement of a user on a device or settings which automatically broadcast a person's contact details. These obligations are particularly relevant considerations for organisations whose products or services are directed at/ intended for, or are likely to be accessed by children⁹². Recital 78 of the GDPR provides examples of measures which controllers may use as part of their data protection by design and default policy. These include *"minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, and enabling the controller to create and improve security features"*. However, this is a non-exhaustive list, and controllers should innovate to develop or

implement other measures which enhance safeguards and ensure the highest level of adherence to data protection principles, bearing in mind the obligation to act in the best interests of child users. The measures should be appropriate to the nature, scope, context and purposes of the processing and the organisation should be able to demonstrate how those measures represent best practice, in particular in making the user environment one which optimises protections and safeguards and minimises to the greatest extent possible, the risks to child users in relation to the processing of their personal data. In considering how to comply with the data protection by design and default obligation with regard to settings, features, and user interactions with services, organisations must objectively and honestly evaluate the underlying processing that is integral to these aspects with regard to the impact that they have on the position of a child user in relation to their personal data. The best interests of a child may not always coincide with an organisation's commercial interests, business model or the objective underlying a service offering. In fact, the best interests of the child principle may seriously conflict with or hamper such objectives. Nevertheless the child user's best interests must prevail in any such commercial decision-making. An organisation should be able to show how the best interests principle has driven the design, development, implementation and/ or operation of any service which is directed at/ intended for, or is likely to be accessed by, children and how measures implemented are effective in achieving this.

7.3 RECOMMENDED MEASURES FOR INCORPORATING DATA PROTECTION BY DESIGN AND BY DEFAULT TO PROMOTE THE BEST INTERESTS OF CHILD USERS

There is no one-size-fits-all solution to data protection by design and default, and what might be deemed appropriate and best practice in this area for one organisation may be completely unsuitable for another organisation.

The following is a list of examples of data protection by design and default measures that the DPC considers appropriate in the context of children (and indeed some will equally apply to adult data subjects). This list merely serves as an indicative selection of measures but it is by no means exhaustive:

DEFAULT PRIVACY SETTINGS – Ensure the strictest privacy settings apply to services directed at/ intended for, or likely to be accessed by, children. For example, where there is an option to make any personal data publicly available, this should not be the default setting. Rather, the user should have to proactively take steps to do so. Where a child switches off a default privacy setting, at the end of a session this should automatically switch back to the default settings.

USER CHOICE – Ensure that in a mixed-audience setting, child users have meaningful, clear and plain choice, control and flexibility as to settings and features in respect of processing operations which pose greater levels of risk to child users and which can be (and are by default – see further below) disabled

WHAT ADULTS THOUGHT...

Restrict/control access to children's personal data by internal members of staff

Opt to process personal data on the child's device, rather than transfer such data to additional systems

Provide layered, child-friendly privacy information that is accessible to children throughout their user experience

Provide clear consent mechanisms which allow children to easily revoke consent at any time

Create, maintain, and uphold policies and technical controls with regard to collection, retention, sharing, etc. of children's personal data

Ensure prominent display of privacy settings on a website or within an app so that a child can access them easily and at any time

Turn off geo-location by default for child users

Ensure strictest privacy settings apply to children by default

Prohibition on delivery of internet-based ads to children identified as under 16

Carry out regular data protection training for all staff

for a child user account (e.g. suggestions for new third-party contacts). Where controls are delegated to parents then they too should default to these lower-risk settings.

DATA MINIMISATION – Minimise the amount of data collected from children in the first instance and throughout their interaction with a service and/or minimise the subsequent use and sharing of the data. Reduce the level of granularity of data types collected from children to avoid specificity and accuracy wherever profiling occurs, could occur or may occur in future.

SHARING AND VISIBILITY – Do not systematically share a child’s personal data with third parties without clear parental knowledge, awareness and control; build in parental reminders/ notifications in relation to subsequent sharing activity. Do not make children’s identity or contact information available to others without parental knowledge, awareness and the opportunity for intervention.

GEOLOCATION – Turn off geolocation by default for child users unless the service being provided is necessarily dependent upon it; if this is the case, make it clear to the child (e.g. through the use of symbols/ icons) that their location is available to the service or can be seen by other users. Provide clearly visible controls to allow the child to change this at any time or following each session, after a short time period, or once the event or feature requiring location has completed. Significantly reduce the level of accuracy of geolocation data collection except where necessary.

PROFILING – Turn off identifiers, techniques or settings which allow any tracking of activity online for advertising purposes (see Section 6).

NUDGE TECHNIQUES⁹⁴ – Avoid the use of nudge techniques that encourage or incentivise children to provide unnecessary information⁹⁵ or to engage in privacy disrupting actions. An example of this might be presenting a large “*Use my contact info*” button in a prominent position on an app screen, followed by a smaller “*Don’t use my contact info*” button underneath or in a less obvious position.

ENCOURAGE PRIVACY-PRESERVING BEHAVIOURS – This can be achieved for example by push notices/ just-in-time notifications emphasising that one or more option(s) provides a greater level of privacy than the action the child user is about to embark on (e.g. switching on features such as location tracking which are automatically set to be off by default) and reminding users about the potential consequences or outcomes of the particular action they are about to take and/or advising them to discuss this with a trusted adult.

BUILT-IN TRANSPARENCY – Provide layered, child-friendly information that is accessible to children throughout their user experience. As with all transparency measures, it should still remain comprehensive and clear, but should also cover the additional precautions, controls, reporting tools, possible or required interventions by the organisation or parent (and their impact) on child accounts.

DEVICE-LEVEL PROCESSING – Opt to process personal data on the user’s device, as opposed to transferring the data to the cloud.

DATA-DRIVEN AUTO FEATURES – Avoid the use of personalised auto-extensions, such as autoplay features and reward loops where children’s

personal data is used to support these features.

USER-SPECIFIC PRIVACY SETTINGS – Privacy settings should be specific to the user rather than a device so as to allow for a child user (e.g. where they use a parent’s device) to benefit from default privacy settings and protections. Consider isolating other aspects of services in child-oriented ways and restricting access to these areas by unrelated adult account holders.

PARENTAL DASHBOARD – Where appropriate, provide parents with an overall view of activity (including any history of activity) and settings that their child has available to them. Child accounts should have available information on the functionality of such dashboards.

PARENTAL TRACKING/ MONITORING – Where service/ device settings allow for parents to track or monitor their child’s use of online services (such as with a parental dashboard, where appropriate), transparency settings should apply so that it is visible to the child that their parent(s) can tell which app/ website/ program etc. they are using or that their parent(s) can later review their activity history.

INTERVENTION – Where service/ device settings allow for parents to track or monitor their child’s use of online services, consider allowing parents to modify child account controls and settings, where appropriate. Provide notifications to parents when these settings are altered, especially where location, biometrics or device sensors are involved. Ensure access to such a dashboard by parents is secured with multiple factors of authentication.

RISK MANAGEMENT – Make consideration of processing of children’s personal data a requirement in all DPIAs. This should include access control restrictions for adults to child audiences or child-oriented areas of a service.

SECURITY – Consideration of children as an audience and the risk factors associated with processing children’s personal data should be a priority when creating, updating or maintaining security controls, measures and “threat models”. This may mean making controls easier to use while maintaining the same high level of security. Alternatively, it may mean making controls only available to parents. Default settings for such controls should ensure high levels of security rather than more relaxed levels that may be available to adults. Higher security settings for child account data may be appropriate, including the possibility of isolating or “air gapping” child personal data from adult personal data. Administrator accounts for child data should be flagged or have a specific role so that internal organisational access can be easily distinguished, monitored, audited and altered.

BREACHES – Notification procedures in cases of personal data breaches should account for notification to the parent rather than the child, where appropriate depending on the age of the child user affected. Breach records maintained by an organisation and notified to the DPC should include references to any involvement of children’s personal data.

BIOMETRICS – Avoid the collection and processing of children’s biometric data.

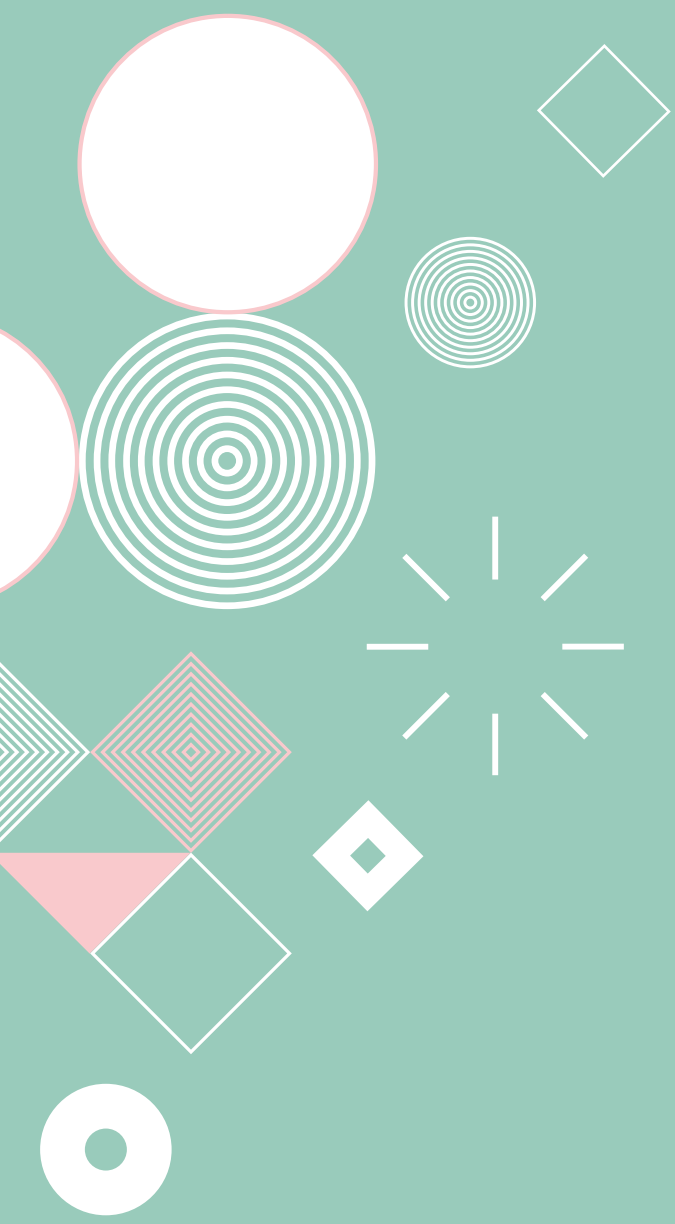
AUDIENCE CONTROL – Where a child can share communications, content or data, ensure limited audience selections by default. Public or open sharing or even limited audience sharing may not be appropriate while sharing only with known “friends” or parents may be possible. Contact from others outside of the child’s authorised contacts should be not possible for younger children

without parental knowledge, awareness and intervention.

ADULT ACCOUNT MIGRATION, RETENTION – Where a child account matures such that parental authorisation/ controls/ intervention no longer apply, personal data associated with that account should not automatically be migrated to a new account or the newly matured status of that account. The user may wish to remove or archive such data, perhaps in full or in part. Likewise, parental control of such accounts should be deactivated or de-linked with mutual operations by the parent and user, rather than unilaterally. Retention of any child account data should also be optional and accounted for by the organisation with the user's confirmed knowledge and awareness. New purposes for the use of retained data must be made clear and explained to the user, who should be offered the chance to reset security and contact details.

CONSISTENCY OF SERVICE – Ensure that measures put in place to protect children are demonstrably effective and that they are equally effective whether a service is delivered by an organisation on a website, mobile device, gaming console or other channel.

CUMULATIVE RISKS – Some risks are cumulative – for example – making a child's profile public and then profiling them for a friend suggestion with an adult user⁹⁶. Together the lack of privacy and the profiling put that child at risk. Organisations should always consider cumulative risk as part of its risk assessment process.



Conclusion

This draft rests heavily on significant consultations, expert input and stakeholder submissions, including from children themselves.

The digital world is central to children's lives and the collection and use of children's data begins at an early age continuing throughout their lifetime. Children as data subjects merit special protections under the GDPR and this document has been produced by the DPC to assist organisations who process children's data by clarifying the standards, arising from these high-level obligations. The DPC has identified 14 core Fundamentals that organisations should follow to enhance protections for children in the processing of their personal data, and has also provided an indicative list of recommended measures for data protection by design and default which should assist in mitigating some of the central risks associated with processing children's personal data.

In addition to the special protections required for the processing of children's data, the Fundamentals prioritise the best interests of the child so that the processing of children's personal data does not interfere with, conflict with or negatively impact, at any level, the best interests of the child. For all users of online services, how personal data is processed, by whom and how this is used, is often complex and opaque. Children cannot be expected to manage this complexity themselves, nor ensure their rights are upheld.

By requiring organisations that routinely process children's personal data to look at controls, choices, settings, features, user options and further use of personal data, amongst other things, in light of the special protections required under the GDPR for children, the DPC considers that this will create safer, more appropriate and more privacy-respecting online environments for children to play, interact, learn and create than currently exists.

CONSULTATION PROCESS

All stakeholders are invited to respond to this document by making submissions/ providing their observations and comments on this document to the DPC by 31 March 2021. Any person who wishes to respond to this consultation process may make submissions/ provide observations and comments on any part of this document and in whatever format they choose to do so.

Any responses should be emailed to childrensconsultation@dataprotection.ie. Alternatively, responses can be sent by post to the following address:

Data Protection Commission
Children's Policy Unit
21 Fitzwilliam Square South
D02 RD28
Ireland

IMPORTANT NOTICE – PUBLICATION OF RESPONSES

IT SHOULD BE NOTED THAT THE DPC INTENDS TO PUBLISH ON ITS WEBSITE THE CONTENT OF ALL RESPONSES RECEIVED TO THIS CONSULTATION. THE IDENTITY OF EACH PARTY RESPONDING WILL LIKEWISE BE PUBLISHED UNLESS THAT PARTY IS AN INDIVIDUAL WHO HAS EXPRESSLY REQUESTED NOT TO BE PUBLICLY IDENTIFIED.

Notes

¹ Section 29 Data Protection Act 2018

² See for example: ZEEKO (2018) Children's online behaviours in Irish primary and secondary schools. Retrieved from: <https://zeeko.ie/wp-content/uploads/2018/06/ZEEKO-TREND-REPORT-.pdf> - p.4

³ For Stream One of the DPC's consultation see: [https://www.dataprotection.ie/en/news-media/latest-news/public-consultation-processing-childrens-personal-data-and-rights-children-;](https://www.dataprotection.ie/en/news-media/latest-news/public-consultation-processing-childrens-personal-data-and-rights-children-)

For Stream Two please see: <https://www.dataprotection.ie/en/news-media/consultations/know-your-rights-and-have-your-say-stream-two-dpcs-public-consultation-processing-childrens-personal>

⁴ For Stream one of our consultation see: <https://www.dataprotection.ie/en/news-media/public-consultation/whose-rights-are-they-anyway> ; For stream two please see <https://www.dataprotection.ie/en/news-media/public-consultation/some-stuff-you-just-want-keep-private-preliminary-report-stream-ii>

⁵ EDPB's Guidelines on Transparency under the GDPR as last revised and adopted on 11 April 2018 (see paragraph 9)

⁶ Article 30.1 of the GDPR provides that each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. Amongst the information required to be kept in the record of processing is a description of the categories of data subjects.

⁷ This non-exhaustive list of factors has been identified by the Federal Trade Commission (FTC) in its role as regulator for enforcing the US Children's Online Privacy Protection Act (COPPA), for the purposes of assisting "operators" in analysing who their "intended audience is, the actual audience, and in many instances, the likely audience for [their] site or service." The FTC will also consider a website or online service to be directed to children if it has "actual knowledge that it is collecting personal information directly from users of another website or online service that is directed to children." See <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Web%20sites%20and%20online>

⁸ The scope of application of these Fundamentals is intended to be consistent (in the context of online services) with the scope of application of the UK Age Appropriate Design Code, in the interests of creating a harmonised network of principles which will apply post Brexit, in circumstances where organisations providing online services in the EU and the UK will be subject to both laws of the UK and separately, the application of the GDPR under EU law.

⁹ <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>. This code requires organisations to either establish age with a level of certainty that is appropriate to the risks to children's rights and freedoms that arise from processing, or apply the standards in this code to all of the organisation's users instead.

¹⁰ Article 42A of the Irish Constitution provides that "The state recognises and affirms the natural and imprescriptible rights of all children and shall, as far as practicable, by its laws protect and vindicate those rights."

¹¹ Council of Europe, European Convention on the Exercise of Children's Rights, 25 January 1996

¹² European Parliament resolution of 16 January 2008: Towards an EU strategy on the rights of the child (2007/2093(INI)) Accessed via: <https://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2008-0012&language=EN>

¹³ For the full text of the UN Convention on the Rights of the Child, please see http://www.childrensrights.ie/sites/default/files/submissions_reports/files/UNCRC_English_0.pdf

¹⁴ All countries in the world have ratified it with the exception of the USA and Somalia: <https://www.gov.ie/en/publication/a1481d-united-nations-convention-on-the-rights-of-the-child/>

¹⁵ For the full text of the European Convention on Human Rights, please see https://www.echr.coe.int/Documents/Convention_ENG.pdf

¹⁶ See *Case C-335/17 Neli Valcheva v Georgios Babanarakis*, 12 April 2018 in which in an Opinion by Advocate General Szpunar it was stated that the CJEU has also already had occasion to point out that the UNCRC binds each of the Member States and is one of the international instruments for the protection of human rights of which it takes account in applying the general principles of EU law. The Advocate General in that case noted at paragraph 37 (referencing a range of case law) that the CJEU has held that the principle of the primacy of the interests of the child is the prism through which the provisions of EU law must be read.

¹⁷ Article 3(3) TEU provides that the "Union shall establish an internal market" and that the Union "shall promote ... justice ..., solidarity between generations and protection of the rights of the child".

¹⁸ For the full text of the Charter of Fundamental Rights of the EU, please see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>

¹⁹ See "Explanation on Article 24 — The rights of the child" section in: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF>

²⁰ The Committee on the Rights of the Child is the body of 18 Independent experts that monitors implementation of the [Convention on the Rights of the child](https://www.ohchr.org/en/hrbodies/crc/pages/crcindex.aspx) by its State parties. See: <https://www.ohchr.org/en/hrbodies/crc/pages/crcindex.aspx>

²¹ The UN Committee stated in 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) that such circumstances may include "age, sex, level of maturity, experience, belonging to a minority group, having a physical, sensory or intellectual disability, as well as the social and cultural context in which the child or children find themselves, such as the presence or absence of parents, whether the child lives with them, quality of the relationships between the child and his or her family or caregivers, the environment in relation to safety, the existence of quality alternative means available to the family, extended family or caregivers, etc." See: <https://archive.crin.org/en/library/publications/un-crc-general-comment-no-14-2013-right-child-have-his-or-her-best-interests.html>

²² The European Data Protection Board (EDPB) is established under Article 68 of the GDPR as an independent EU body which contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

²³ Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), 398/09/ EN WP 160: "The rationale of this principle is that a person who has not yet achieved physical and psychological maturity needs more

protection than others. Its purpose is to improve conditions for the child, and aims to strengthen the child's right to the development of his or her personality. This principle must be respected by all entities, public or private, which make decisions relating to children. It also applies to parents and other legal representatives of children, either when their respective interests are in conflict, or where the child is being represented. Normally, the child's representatives should apply this principle, but where there is a conflict between the interests of children and their legal representatives, the courts or, where appropriate, the DPAs (Data Protection Authorities) should decide."

²⁴ See: <https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx>

²⁵ Recital 58 of GDPR, The principle of transparency, focuses on presenting information in a clear, concise and easily accessible and easy to understand way. In relation to children, the recital says 'any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.'

²⁶ Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) 398/09/EN WP 160

²⁷ This reflects the position of the EDPB's Guidelines on Transparency under the GDPR as last revised and adopted on 11 April 2018 (see paragraph 35)

²⁸ For more information on certain circumstances where individual rights may be restricted see:

<https://www.dataprotection.ie/en/individuals/know-your-rights/restriction-individual-rights-certain-circumstances>

²⁹ For more detailed information on legal bases, please see the DPC's dedicated guidance note on Legal Bases for Processing Personal Data. Available at:

https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf

³⁰ See EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, page 5.

³¹ See "Contract Law" (2nd ed.) Paul A. McDermott and James McDermott (Bloomsbury Professional, 2017) at Chapter 18

³² This concept is defined under both Section 2 of the Sale of Goods Act 1893 as "goods suitable to the condition in life of such infant or minor... and to his actual requirements at the time of sale and delivery" and also under common law to include items such as food and drink; clothing; board and lodging; transport; medical assistance; legal aid; contracts for necessary services (ibid).

³³ See "Contract Law" (2nd ed.) Paul A. McDermott and James McDermott (Bloomsbury Professional, 2017) at Chapter 18

³⁴ The GDPR identifies children in particular as "vulnerable natural persons" in Recital 75

³⁵ EDPB's Guidelines on Transparency under the GDPR as last revised and adopted on 11 April 2018 (see paragraph 15)

³⁶ Ibid (see paragraph 7)

³⁷ This approach is consistent with the following recommendation made by the UN Committee on the Rights of the Child in its Report of the 2014 Day of General Discussion on "Digital media and children's rights" (2014), paragraph 103: "States [should] ensure that all children have meaningful and child-friendly information about how their data is being gathered, stored, used and potentially shared with others. In this regard, States should ensure that age-appropriate privacy settings, with clear information and warnings, are available for children using digital media and ICTs".

³⁸ Anna Morgan, The Transparency Challenge: Making children aware of their data protection rights and the risks online (2018) Available at: <https://www.dataprotection.ie/sites/default/files/uploads/2019-02/TransparencyChallenge.pdf> p.3

³⁹ See for example comments on children's lack of awareness of commercial privacy and data collection practices in Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science.

⁴⁰ Section 29 Data Protection Act 2018

⁴¹ For more information please see: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/>

⁴² "Some stuff you just want to keep private!" Preliminary report on Stream II of the DPC's consultation on the processing of children's personal data and the rights of children as data subjects under the GDPR", Data Protection Commission (2019) available at: https://www.dataprotection.ie/sites/default/files/uploads/2019-08/Some%20Stuff%20You%20Just%20Want%20to%20Want%20to%20Keep%20Private_Consultation%20Report.pdf

⁴³ General Comment No. 12 (2009) The Right of the Child to be Heard - see paragraph 20 - 21

⁴⁴ This also arises from the regulations restricting the right of access to medical data (S.I. 82/1989 Data Protection (Access Modification) (Health) Regulations 1989, as amended) and social work data (S.I. 83/1989 Data Protection (Access Modification) (Social Work) Regulations 1989, as amended) which prohibit the release of such data where it would be likely to cause serious harm to the physical or mental health of a person and which also require that where such data is held other than by a medical practitioner, or a social worker, as applicable, that it not be released without the data controller first consulting the relevant medical practitioner or social worker.

⁴⁵ Similarly, in its 2018 Recommendation CM/Rec (2018) 7 of the Committee of Ministers to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, the Council of Europe highlighted that "States and other stakeholders should ensure that children are made aware of how to exercise their right to privacy and data protection, taking into account their age and maturity and, where appropriate, with the direction and guidance of their parents, carers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child".

⁴⁶ Article 3 of the UNCRC acknowledges the rights and duties of the parents, legal guardians or other individuals legally responsible for a child and Article 5 guarantees respect for the responsibilities, rights and duties of parents/ legal guardians "to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights which are set out in the UNCRC." Notably, Article 16 of the UNCRC protects the child against arbitrary or unlawful interferences with his or her privacy. Finally, relevant to the current issue is Article 12 of the UNCRC which protects the right of a child who is capable of forming his or her own views, to express those views freely in all matters affecting himself or herself, with due weight being given to the child's views in accordance with the age and maturity of the child.

⁴⁷ As the OCO submitted in its response to the DPC's 2019 consultation, there are children and young people who, for age and/or other reasons affecting their capacity, will not be able to make an access request themselves and who

will therefore be dependent on a parent/ guardian to make an access request and to exercise their right of access on their behalf. Equally, the OCO points out that there are also children and young people who will have the capacity to make an access request themselves, but who *may prefer* their parent/guardian to do so on their behalf or who may want to jointly make an access request. See: <https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Submission%20from%20Ombudsman%20for%20Children%27s%20Office.pdf>

⁴⁸ In the case of *Mck v The Information Commissioner* [2006] IESC 2, which concerned access under the Freedom of Information Act 1997 which was in force at the time, the Supreme Court held that “*The [FOI] Act of 1997 and the Regulations fall to be interpreted in accordance with the Constitution. A parent ... has rights and duties in relation to a child. It is presumed that his or her actions are in accordance with the best interests of the child. This presumption while not absolute is fundamental...*”

⁴⁹ This list of factors is based in the main on existing guidance from the Office of the Information Commissioner (OIC) in Ireland in relation to requests for access by a parent or guardian to a child’s records made under the Irish Freedom of Information Act 2014. See <https://www.oic.ie/guidance-and-resources/guidance-notes/1-Section-37-Guidance-Note.pdf> pp.35-39

⁵⁰ Article 4(25) GDPR references Directive 2015/1535 by way of the definition of the term “information society service”: “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.” The CJEU has ruled that the concept of remuneration does not apply solely to payments given by the recipients of the service and can apply to situations where the payment is made by another party (*Case-352/85 Bond van Adverteerders and Others v The Netherlands State* [1988] E.C.R 2085).

⁵¹ Article 8 of the GDPR allows for Member States to legislate nationally for the age at which children can legally consent to the processing of their own personal [data in an online context](#), as long as it is between 13 and 16 years of age. The default position where a Member State has not passed its own laws on this issue is that the age of 16 applies. In Ireland, after much public debate, 16 years was set as the age of digital consent under Section 31 of the Data Protection Act 2018, with the proviso that a review of this age limit be concluded within 4 years (i.e. by May 2022).

⁵² In accordance with Article 7.3 GDPR

⁵³ See the EDPB [updated] Guidelines 05/2020 on Consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, Section 7

⁵⁴ The FTC has published a “Six Step Compliance Plan” to help online service operators in the US ensure that they fulfil the requirements of the COPPA rule. Step four of this plan sets out a series of acceptable methods for obtaining verifiable consent from parents before collecting personal data from their children.

⁵⁵ Under the [Children’s Online Privacy Protection Act \(COPPA\)](#)

⁵⁶ Please see:

<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule>

⁵⁷ This practical implication of Article 8 is reflected in guidance by the EDPB on consent under the GDPR Guidelines 05/2020 on consent under Regulation 2016/679, which states that: “*When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities [...] Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor. If doubts arise the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required.*”

⁵⁸ For example, Google noted in its submission that “*In many cases, [children] may be relying on these online service providers as their primary vehicle for access to important educational content and information. Thus, the unintended consequence of locking out users is that [...] they could be deprived of not only access to the service, but access to important content and information that they have stored online such as homework assignments*” see:

<https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Submission%20from%20Google.pdf>

Technology Ireland also noted that “*Locking users out of services may deprive data subjects of the tools they use to access information or educational resources they need for school, as well as records of prior activity —such as documents or pictures — that they may want to retain.*” See:

<https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Submission%20from%20Technology%20Ireland.pdf>

⁵⁹ Under Article 12 of the UNCRC

⁶⁰ Under Article 13 of the UNCRC

⁶¹ Research by CyberSafeIreland has found that 60% of children aged 8-13 are using social media and messaging platforms despite being under the stipulated minimum age. CyberSafeIreland has also argued that “*It is likely children in general are now more vulnerable online [...] as a greater proportion of them are incentivised to lie about their age to avoid additional GDPR constraints for 13-16 year olds.*” See: https://cybersafeireland.org/media/1300/csi_annual_report_2018_w.pdf pp. 20-21.

⁶² “*I wasn’t sure it was normal to watch it”: A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people.* NSPCC, Children’s Commissioner and Middlesex University London. May 2017.

⁶³ Some of these criteria take into account certain suggestions which were submitted by participants as part of their responses to the DPC’s public consultation.

⁶⁴ It should be noted that while Section 30 of Data Protection Act 2018 stipulates that it shall be an offence to process the personal data of a child for the purposes of direct marketing, profiling, or micro-targeting, this provision has not been commenced. For more information please see:

<https://www.oireachtas.ie/en/debates/question/2018-07-24/623/?highlight%5B0%5D=623>

⁶⁵ Article 29 Data Protection Working Party, ‘Opinion 02/2013 on Apps on Smart Devices, WP202’ (2013) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

⁶⁶ EDPB Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (2018), page 29

⁶⁷ Opposition to the profiling of children was expressed by the Council of Europe in its 2018 Recommendation to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (Recommendation CM/Rec 2018(7)) at page 17:

Profiling of children, which is any form of automated processing of personal data which consists of applying a “profile” to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour or attitudes, should be prohibited by law. States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.

⁶⁸ It may also involve the promotion of the ethos of an organisation or the canvassing of votes in the context of an election or a referendum.

⁶⁹ This statutory instrument transposes in Ireland the rules set out in Directive 2002/58/EC as amended by Directive 2006/24/EC and Directive 2009/136/EC (known as the E-Privacy Directive)

⁷⁰ Consent under the ePrivacy Regulations must be interpreted in line with the definition of consent in Article 4(11) of the GDPR in accordance with Article 94 GDPR, in other words it must be: *“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (emphasis added)”*.

⁷¹ See the EDPB [updated] Guidelines 05/2020 on Consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020, Section 1, paragraph 7

⁷² As previously noted, Directive (EU) 2015/1535 defines the term “information society service” at Article 1 as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.” The phrase “electronic means” according to Article 1 “means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means”. Annex 1 of that Directive explicitly excludes “telephone/telex direct marketing” from the definition of “information society services” by stating that these are not services provided by “electronic means”.

⁷³ Recital 18 of the E-Commerce Directive (Directive 2000/31/EC) states that “information society services” is intended to “those offering online information or commercial communication”. EU case law has indicated that “commercial communication” includes advertising and marketing. Moreover, Advocate General Bot suggested in his Opinion in Case C-339/15 *Openbaar Ministerie v Luc Vanderborght* (ECJ, 8 September 2016) that the EU Commission intended for online direct marketing services to fall within the scope of “information society services” (see footnote 25).

⁷⁴ More information on these rules can be found in the DPC’s guidelines on direct marketing. See: <https://www.dataprotection.ie/en/organisations/rules-electronic-and-direct-marketing>

⁷⁵ The DPC also notes Article 19(4) of the International Chamber of Commerce Advertising and Marketing Communications Code which states that *“Personal data collected from children should not be used to address marketing communications to them, the children’s parents or other family members without the consent of the parents.”*

⁷⁶ Regulation 13(11) of the ePrivacy Regulations allows for direct marketing in the context of the sale of a product or a service, where certain conditions are met, but does not specifically require affirmative consent. <https://www.dataprotection.ie/en/organisations/rules-electronic-and-direct-marketing>

⁷⁷ Article 4(4) of the GDPR defines profiling as: *“[A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”*

⁷⁸ Other examples include: decisions that affect someone’s financial circumstances, such as their eligibility to credit; decisions that affect someone’s access to health services; decisions that deny someone an employment opportunity or put them at a serious disadvantage; decisions that affect someone’s access to education, for example university admissions. See EDPB Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (2018), page 21 - 22.

⁷⁹ Article 22(2) outlines a number of exceptions to this restriction on profiling: where it is (a) necessary for the performance of a contract; (b) authorised by EU or Member State law, or; (c) based on the explicit consent of the data subject. However, where these exceptions apply, Article 22(3) obliges controllers to put in place safeguards to protect the data subject’s rights, freedoms and legitimate interests, including “the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.” Recital 71 sheds further light on the nature of these safeguards, adding that they should include the provision of specific information to the data subject, an explanation of the decision reached and an opportunity to challenge the decision in question. Article 22(4) prohibits profiling based on special categories of personal data (e.g. racial, ethnic or religious personal data) with limited exceptions, such as where it is based on explicit consent and is authorised by EU or member state law. It should also be noted that controllers are obliged under Article 14(2) to inform data subjects if they are subject to any automated decision making including profiling and to provide “meaningful information” on the logic involved as well as the significance and the envisaged consequences of this processing.

⁸⁰ EDPB Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (2018), page 28

⁸¹ See the DPC’s Guidance Note (April 2020) on Cookies and other Tracking Technologies at: <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20other%20tracking%20technologies.pdf>

⁸² Sonia Livingstone et al., “Children’s data and privacy online: growing up in a digital age: research findings (2019) <http://eprints.lse.ac.uk/101282/>

⁸³ Karen Mc Cullagh, “The general data protection regulation: a partial success for children on social network sites?” *Data Protection, Privacy and European Regulation in the Digital Age* (2016), p. 117

⁸⁴ There is a growing body of research that underlines the ethical implications of serving targeted online advertisements to children due to their vulnerability, their still-evolving capacity to distinguish targeted advertising from other online content, and the asymmetries of power between child consumers and the digital advertising sector. A study by Reijmersdal et al. found that *“Children are unaware of the tactics used in profile targeting, which makes them vulnerable to persuasion. They are unable to recognize profile-based targeting of either the product or form, and [they] need help understanding this new marketing*

technique." See: Eva A. van Reijmersdal, Esther Rozendaal, Nadia Smink, Guda van Noort & Moniek Buijzen (2017) Processes and effects of targeted online advertising among children, *International Journal of Advertising*, 36:3, 396-414, DOI: [10.1080/02650487.2016.1196904](https://doi.org/10.1080/02650487.2016.1196904)

⁸⁵ Organisations may also wish to consider the "Children's Rights Business Principles" (CRBP), a set of guiding principles created by UNICEF, the UN Global Compact and Save the Children to help businesses ensure that their activities respect children's rights in international law. In particular, Principle 6 of the CRBP states that businesses should use "marketing and advertising that respect and support children's rights." In practice, this means controllers should avoid marketing that has an adverse effect on the child, including through exploiting "children's greater susceptibility to manipulation, and the effects of using unrealistic or sexualized body images and stereotypes". This aligns with the principle that the best interests of the child must always be paramount. See:

https://www.unglobalcompact.org/docs/issues_docdoc/human_rights/CRBPCRBP/Childrens_Rights_and_Business_Principles.pdf

⁸⁶ This aligns with the views of the EDPB that solely automated decision making including profiling which produces legal or similar effects should not be used for children and the exceptions to the rule against this form of processing should not be relied on in relation to processing children's data other than limited circumstances such as where it is necessary to protect their welfare. See *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (2018), page 28

⁸⁷ See EDPB *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, wp248rev.01

⁸⁸ *"Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data)".* (Paragraph 7, page 10)

⁸⁹ For more information please see:

<https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf>

⁹⁰ For example see the Swedish Data Protection Authority's list of processing operations requiring a DPIA:

<https://www.datainspektionen.se/globalassets/dokument/beslut/list-regarding-data-protection-impact-assessments.pdf>

⁹¹ This position is supported by academics such as Professor Eva Lievens and Simone van der Hoff, who have argued that Article 3 UNCRC requires that in all actions concerning children, their best interests should be the primary consideration and that this principle requires governments, public and private bodies to conduct child (rights) impact assessments and evaluate the impact of any proposed law, policy or decision on children's rights. They argue that this requirement, in itself, provides a strong incentive to assess the risks to children's rights resulting from the processing of their personal data. For more information please see: Simone, van der Hof and Lievens, Eva, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR* (2017). *Communications Law* 2018, Vol. 23, No. 1, Available at SSRN: <https://ssrn.com/abstract=3107660>

⁹² Article 25.2 states that *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*

⁹³ Lievens and van der Hof consider that *"[s]ince children are a dedicated category of individuals demanding stricter data protection under the GDPR, the principles of data protection by design and default seem particularly apt to encourage and ensure the protection of their personal data and, at the same time, their rights more generally are guaranteed."* Please see: Simone, van der Hof and Lievens, Eva, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR* (2017). *Communications Law* 2018, Vol. 23, No. 1, Available at SSRN: <https://ssrn.com/abstract=3107660>

⁹⁴ This is a concept identified in the ICO's Age-Appropriate Design Code which the DPC endorses.

⁹⁵ The ICO's definition of nudge techniques is as follows: *"Nudge techniques are design features which lead or encourage users to follow the designer's preferred paths in the user's decision-making.* The ICO also consider nudge techniques to include making one option much less cumbersome or time-consuming than the alternative, therefore encouraging many users to just take the easy (often more privacy-intrusive) option. They use the example of *"providing a low privacy option instantly with just one "click", and the high privacy alternative via a six-click mechanism, or with a delay to accessing the service."*

⁹⁶ For example see: www.riskyby.design/introduction

APPENDIX 1 – GLOSSARY OF TERMS

TERM:	ORDINARY MEANING / RELEVANT GDPR OR 2018 ACT PROVISION
2018 Act	Data Protection Act 2018 (an Irish act to give further effect at national level to the GDPR)
Age of digital consent	The term commonly used to describe the minimum age in each EEA Member State at which online service providers can rely on a child's own consent to process their personal data in the context of using an online service, without needing the consent of their parent or guardian. (See Article 8 GDPR)
Automated decision-making	The process of making a decision about an individual based on their personal data by automated means, i.e. using software configured to analyse the personal data provided and follow set rules to reach decisions without human involvement. (See Article 22 GDPR)
Biometric data	Personal data which is derived from specific technical processing of the physical, physiological or behavioural characteristics of a person, which allow or confirm the unique identification of that person, such as facial or fingerprint data (see Article 4(14) GDPR)
Child	In Ireland, for data protection purposes, a child is somebody under the age of 18, which is in keeping with the definition of a child under the UNCRC as "a person under the age of 18 years" (see Section 29 of the 2018 Act)
'Connected' devices	A group of devices connected to each other and, usually, connected to a remote server through wired or wireless networks, often collecting and sharing data within the network.
Cookie	A cookie is usually a small text file stored on a device, such as a PC, a mobile device or any other device that can store information. Devices that may use cookies also include so-called 'Internet of Things' (IoT) devices that connect to the internet.

APPENDIX 1 – GLOSSARY OF TERMS

TERM:	ORDINARY MEANING / RELEVANT GDPR OR 2018 ACT PROVISION
Data controller	A person, organisation, or other body that alone, or jointly with others, determines the purposes and the means of the processing of personal data, in other words, which decides how and why a data subject's personal data are processed (see Article 4(7) GDPR)
Data minimisation	The principle of only collecting the minimal amount of relevant personal data necessary to the purpose for which it is being processed (see Article 5(1)(c) GDPR)
Data processing	Using personal data and doing anything with it, from collecting it to storing it, retrieving it, consulting it, sharing it with someone else, erasing it and destroying it (see Article 4(2) GDPR)
Data subject	An identified or identifiable person to whom personal data relates (see Article 4(1) GDPR)
Electronic direct marketing	The promotion of a product or service through emails, texts, faxes, or telephone calls. (see Regulation 13 of the ePrivacy Regulations)
EPrivacy Regulations	SI 336/ 2011 (an Irish statutory instrument transposing Directive 2002/58/EC as amended by Directive 2006/24/EC and Directive 2009/136/EC (known as the E-Privacy Directive)
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679 (an EU law)

APPENDIX 1 – GLOSSARY OF TERMS

TERM:	ORDINARY MEANING / RELEVANT GDPR OR 2018 ACT PROVISION
Geolocation data	Data taken from a user's device indicating the location of that device, including GPS data or data about connection with local Wi-Fi equipment.
Nudge techniques	Design features which lead or encourage users to follow the designer's preferred paths in the user's decision-making. These can include making one option much less cumbersome or time-consuming than the alternative, therefore encouraging many users to just take the easy (often more privacy-intrusive) option.
Online service provider	A company or organisation that provides services hosted on or accessible through the internet.
Personal data	Any information relating to an identified or identifiable person (see Article 4(1) GDPR)
Profiling	A way of using someone's personal data to predict or analyse characteristics about that person, such as services they will be interested in, their likes or dislikes, preferences, views or opinions, or their behaviour, amongst other things. (See Article 4(4) GDPR)
Targeted/ behavioural/ personalised advertising	The practice of using someone's personal data (including a profile which has been built about them) to tailor advertisements and marketing materials, amongst other things, to their interests, needs or individual views.

APPENDIX 2 – ARTICLES AND RECITALS REFERENCED IN THE FUNDAMENTALS RELEVANT TO THE SPECIFIC PROTECTION OF CHILDREN IN THE GDPR

SPECIFIC REFERENCES TO CHILDREN HAVE BEEN EMPHASISED IN BOLD TEXT AND ELLIPSES INDICATED BY (...)

ARTICLE	TEXT
Article 4(4), (11), (25) – Definitions	<p>For the purposes of this Regulation:</p> <p>(...)</p> <p>(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;</p> <p>(...)</p> <p>(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;</p> <p>(...)</p> <p>(25) ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;</p> <p>(...);</p>
Article 5 - Principles relating to processing of personal data	<p>1. Personal data shall be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);</p>

ARTICLE

TEXT

Article 5 - Principles relating to processing of personal data

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6 - Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, **in particular where the data subject is a child.**

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

ARTICLE

TEXT

Article 6 – Lawfulness of processing

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

ARTICLE

TEXT

Article 7 – Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8 – Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, **the processing of the personal data of a child shall be lawful where the child is at least 16 years old**. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, **in particular for any information addressed specifically to a child**. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

ARTICLE

TEXT

Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

ARTICLE

TEXT

Article 13 - Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

ARTICLE**TEXT****Article 14 –
Information to be
provided where
personal data have
not been obtained
from the data subject**

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (e) the right to lodge a complaint with a supervisory authority; (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2: (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

ARTICLE

TEXT

Article 14 – Information to be provided where personal data have not been obtained from the data subject

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 17 – Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; **(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).**

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

ARTICLE	TEXT
<p>Article 17 – Right to erasure ('right to be forgotten')</p>	<p>3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.</p>
<p>Article 21 – Right to object</p>	<p>1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.</p> <p>2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.</p> <p>3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.</p> <p>4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.</p> <p>5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.</p> <p>6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.</p>

ARTICLE	TEXT
<p>Article 22 – Automated individual decision-making, including profiling</p>	<p>1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.</p> <p>2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.</p> <p>3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.</p> <p>4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.</p>
<p>Article 24 – Responsibility of the controller</p>	<p>1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.</p> <p>2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.</p> <p>3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.</p>
<p>Article 25 – Data Protection by Design and Default</p>	<p>1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the</p>

ARTICLE	TEXT
<p>Article 25 – Data Protection by Design and Default</p>	<p>necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.</p> <p>2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.</p> <p>3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.</p>
<p>Article 35 – Data protection impact assessment</p>	<p>1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.</p> <p>2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.</p> <p>3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.</p> <p>4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.</p> <p>5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.</p>

ARTICLE

TEXT

Article 35 – Data protection impact assessment

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

**Article 57(1)
(b) – Tasks of the supervisory authority**

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. **Activities addressed specifically to children shall receive specific attention;**

RECITAL	TEXT
<p>Recital 38</p>	<p>Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.</p>
<p>Recital 47</p>	<p>The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.</p>
<p>Recital 58</p>	<p>The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.</p>

RECITAL

TEXT

Recital 65

A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. **That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.** However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

Recital 70

Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

Recital 71

The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is **based solely on automated processing and which produces legal effects** concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance

RECITAL

TEXT

Recital 71

with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. **Such measure should not concern a child.**

Recital 75

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; **where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.**

