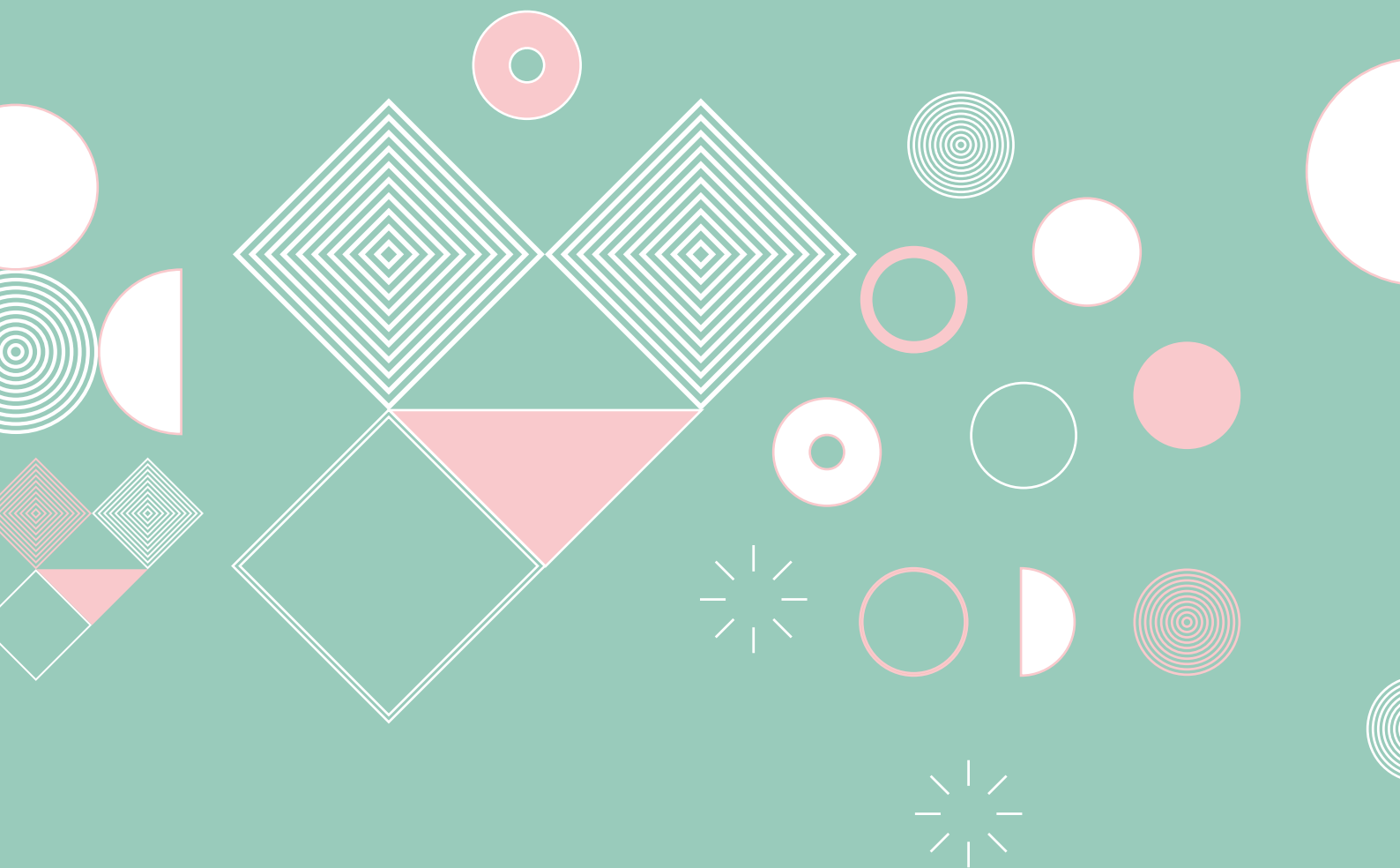
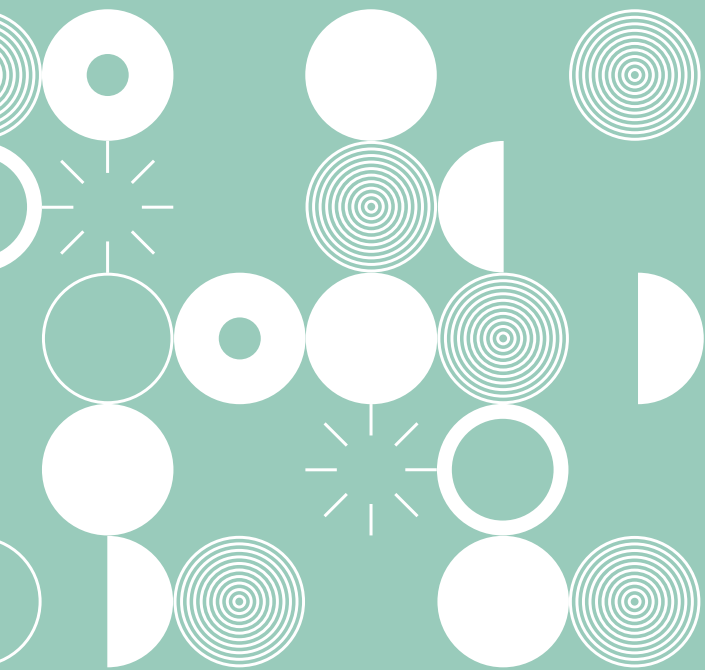


Data Protection Commission

Whose Rights Are They Anyway?

Trends and Highlights from
Stream 1 of the DPC's Public
Consultation on Children's
Data Protection Rights

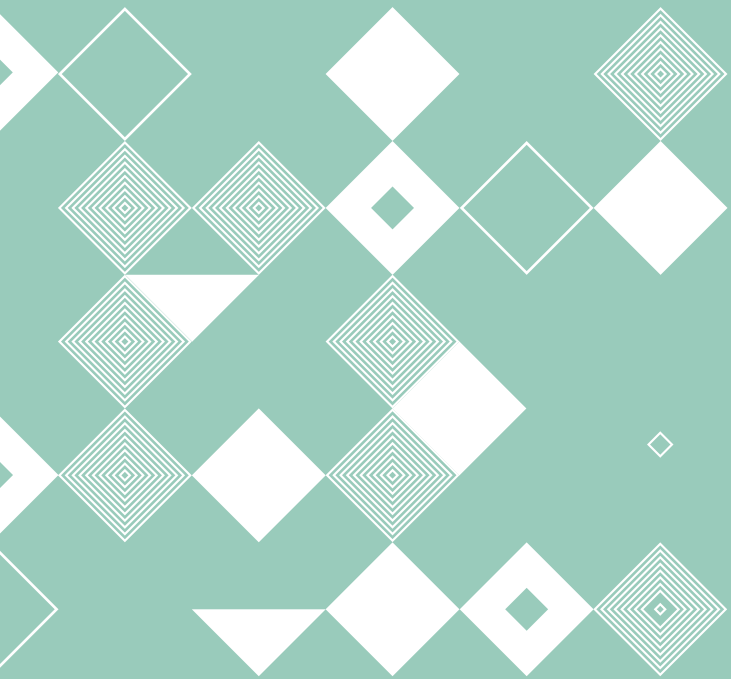




Contents



Introduction	4
Format of the consultation	5
Responses – High-level trends	6
1. Children as data subjects and the exercise of their data protection rights	9
Transparency and the right to be informed	10
Child-specific privacy notices	11
Exercise of data protection rights	12
Alternatives to age-based factors	13
Parental involvement	13
II. Safeguards	15
Age verification methods	16
Withdrawing access to online services offered pre-GDPR to children under the age of digital consent	18
Online service providers and different national ages of digital consent in the EU (Article 8 GDPR)	18
III. Profiling and marketing activities concerning children (Articles 21-22 GDPR)	19
Profiling children for marketing purposes	20
IV. Data protection by design and by default (Article 25 GDPR)	22
Built-in privacy settings for children	23
V. General	25
Conclusion	26



Introduction



INTRODUCTION

From December 2018 to April 2019, the Data Protection Commission ('DPC') ran a public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation ('GDPR'). This consultation was launched in an effort to address a number of questions arising in the context of new child-related provisions under the GDPR, which is the first EU data protection law to highlight the importance of the protection of children's personal data and the position of children as data subjects.

The objective of this consultation 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. The feedback from this consultation will assist the DPC in producing guidance material on the subject of children and data protection.

This will include a detailed piece of guidance aimed at data controllers and interested parties, as well as a separate piece of child-friendly guidance, which will enable children to understand not only the risks that may arise when they supply their personal data online, but also their rights under data protection law. In addition, arising from the consultation, the DPC will also work with industry, government and voluntary sector stakeholders and their representative bodies to encourage the drawing up of codes of conduct (as required under Section 32 of the Irish Data Protection Act 2018).

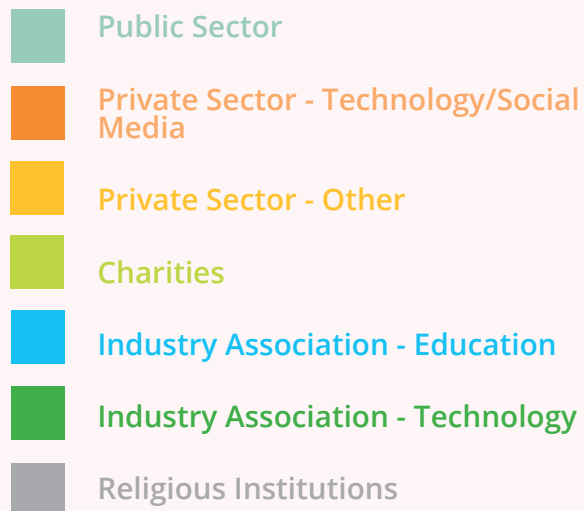
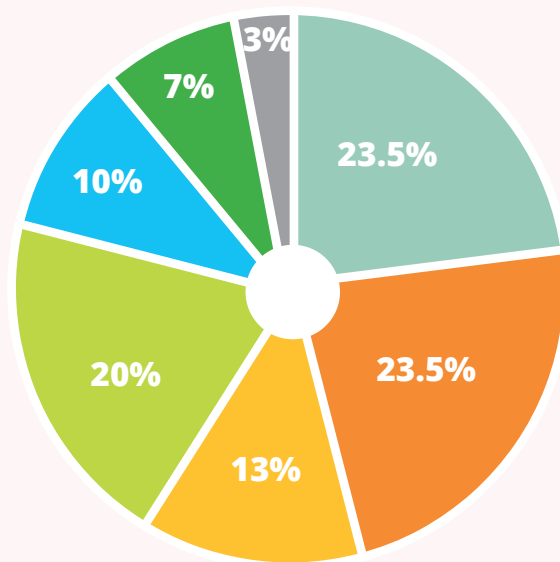
FORMAT OF THE CONSULTATION

The consultation was divided into two streams: One stream brought children and young people directly into the debate by gathering their views in the classroom using a specially designed lesson plan, which was rolled out in schools and Youthreach centres across the country. The other stream – the subject of this report – was focused on adult stakeholders. The DPC invited all interested parties – including, parents, educators, children's rights organisations, child protection organisations, representative bodies for parents and educators, as well as organisations that collect and process children's data – to submit their responses to any or all of the 16 questions set out in the dedicated consultation document. Respondents were free to answer as many of the questions as they wished, and there was no maximum length or word count required.

RESPONSES – HIGH-LEVEL TRENDS

In total, 30 submissions were received in response to this stream of the consultation. Participating stakeholders came from a wide range of sectors, including technology and social media companies, children's rights charities, public sector bodies, academia and trade associations. The DPC was encouraged by the spread in submissions received across private, public and civil society groups in this consultation.

**STREAM 1 SUBMISSIONS
BY STAKEHOLDER CATEGORY**

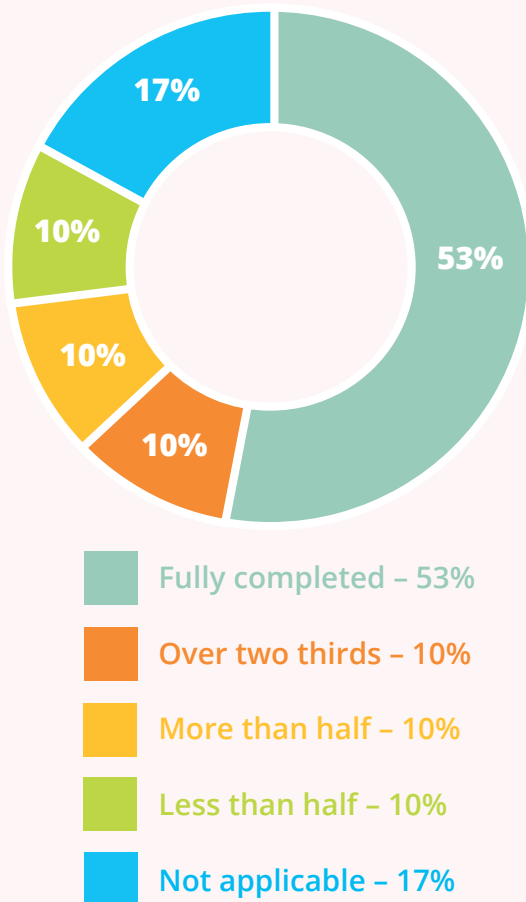


Submissions were received from the following stakeholders (these submissions will also be made available on our website)

- The Teaching Council
- AllOne Corporate Solutions
- Scouting Ireland
- Barnardos
- Minister for Justice and Equality
- SuperAwesome
- Church of Ireland
- Irish Society for the Prevention of Cruelty to Children
- The Pokémon Company International
- The Irish Play Therapy Association
- Group of academics
- The Ombudsman for Children's Office
- ProPrivacy Ltd.
- The Irish Wheelchair Association
- The Irish Heart Foundation
- National Council for Curriculum and Assessment (NCCA)
- Joint Managerial Body
- Department of Education and Skills
- Google
- Department of Public Expenditure and Reform
- TUSLA Child & Family Agency
- Three Ireland
- Early Childhood Ireland
- Technology Ireland
- CyberSafe Ireland
- The Software & Information Industry Association (SIIA)
- Facebook Ireland
- Castlebridge
- Snap Inc.
- Microsoft

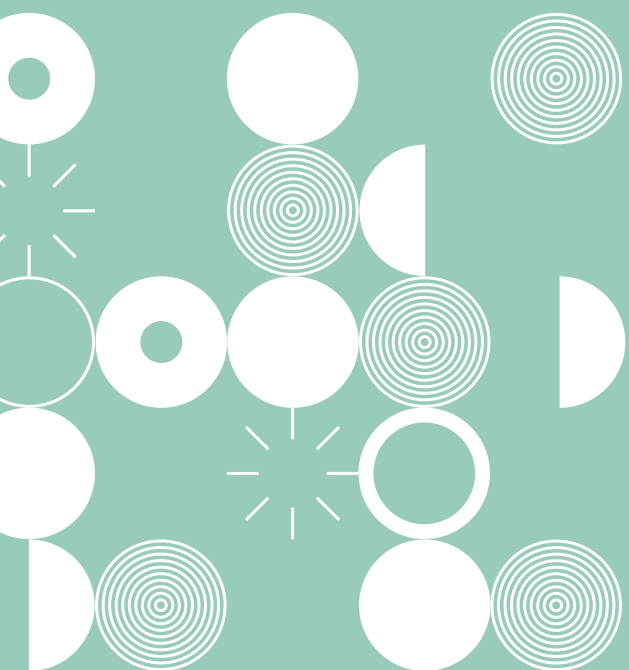
There was a high level of engagement with each of the 16 questions posed in this consultation. As the chart below indicates, almost three quarters of submissions answered at least 9 of the 16 questions in the consultation document, and only 10% of participants answered fewer than half. Some respondents opted not to answer the questions directly and instead submitted essay-style responses that addressed the general themes of the consultation in the order they saw fit. However, many of these freeform submissions broadly addressed numerous questions and provided plenty of valuable insight.

PERCENTAGE OF QUESTIONNAIRE COMPLETED



Another interesting trend was the manner in which participants answered the questions put to them. About two thirds of respondents opted for a prescriptive approach, in which their answers consisted of arguments and research in favour of a particular course of action. This method was particularly popular among individuals and organisations with more academic or research-oriented expertise in children's rights such as industry associations and certain categories of public sector organisations. Others opted for a descriptive approach, in which they presented their own organisation's procedures for addressing the various issues raised in the consultation questions. This was more popular among certain charities and technology companies that engaged with or offered services directly to children.

This report provides an overview of the responses received to each of the 16 questions set out in the consultation document. Due to the open-ended nature of the questions asked and the comprehensive replies of many of the respondents, the trends and themes presented in the rest of this report will be primarily qualitative in nature and will focus on summarising the main positions and views provided by stakeholders to each question.



Children as data subjects and the exercise of their data protection rights



1. Children as data subjects and the exercise of their data protection rights

Transparency and the right to be informed

The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by an organisation (the obligation on an organisation to give this information is known as transparency) and that this information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is stated to be particularly important where such information is being provided to children.

The transparency information that must be provided where an organisation is processing an individual's personal data includes the identity and contact details of the organisation who is collecting or using the personal data, the purposes and the justification (known as 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.

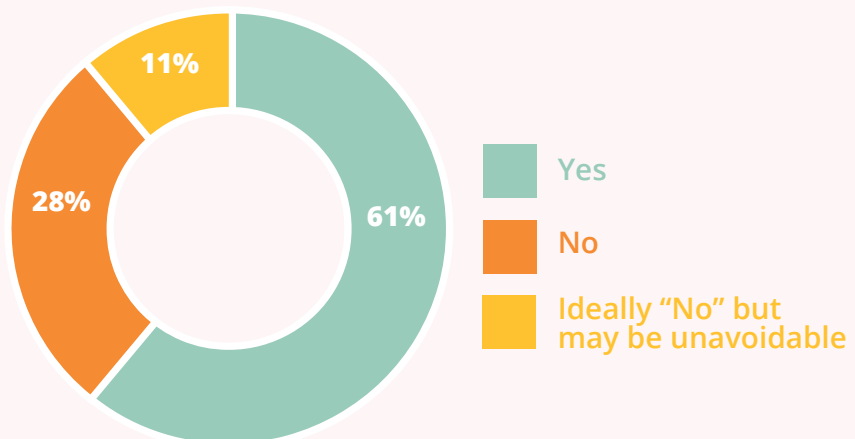
When asked what methods organisations should use to easily convey transparency information to children, virtually all submissions stated that information notices need to be more child friendly. The general view was that messages aimed at children should use either simple language or – in the case of very young children in particular – audio, graphic and other forms of communication appropriate to the age and level of cognitive development of the child. Those in favour of non-textual methods for conveying this transparency information – such as audio or video messages, visual cues, and gamification – generally made one of two arguments: The first was that these methods are more innovative and would help children who are still developing reading capabilities to understand the message being conveyed. For example, one submission suggested creating an “awareness video” consisting of a *“digital footprint cartoon video of a polar bear leaving footprints of data for everyone to see [including a] consent explanation and overview of the consequences.”* Others argued that it is important for controllers to be able to provide transparency information in a manner that is most relevant to the users of their platform or service. For example, one social media platform whose users interact mainly through sharing images and video stated that they created a privacy video to inform users how their data is used, and they displayed this video on users' news feeds and in their support centre, as opposed to providing this information in a lengthy written privacy notice. The same submission referenced the effectiveness of child-friendly images, icons, summaries and just-in-time notices.

Another popular suggestion was that organisations should encourage parental involvement in the transparency piece, either through consent forms detailing what is happening with a child's personal data, or fostering dialogue between parents and children on data protection issues by encouraging children to speak with their parent/guardian if there is anything they don't understand in a privacy policy or information notice. Proponents of this idea came from a wide range of backgrounds including private companies, the public sector, representative bodies and religious organisations. Some pointed out that child-friendly notices would also be popular with adults as they are easier to understand than lengthy and legalistic privacy notices. These could help parents talk to their children about data protection by giving them a better sense of what personal data is and how it is processed. There were also calls for the creation by organisations of more educational resources to help inform children about technology, safety and privacy issues. The DPC's lesson plan for children and young people as part of the second stream of this consultation was cited by one submission as a good example of this. Others proposed that organisations with the means to do so should create their own information booklets for children. Finally, layered privacy notices, which could be adjusted to the maturity of the user, also came up as suggestions in several submissions.

Child-specific privacy notices

The question of whether two sets of privacy notices (one for children and one for adults) should be required for organisations, which offer services to both adults and children, proved divisive. Charities and public sector organisations tended to be in favour of this proposal whereas technology companies tended to be opposed to it. Those in favour emphasised the importance of supplying tailored information that can be understood by all users of a product or service. However, some stakeholders also expressed concern that this requirement could create an unnecessary burden for organisations.

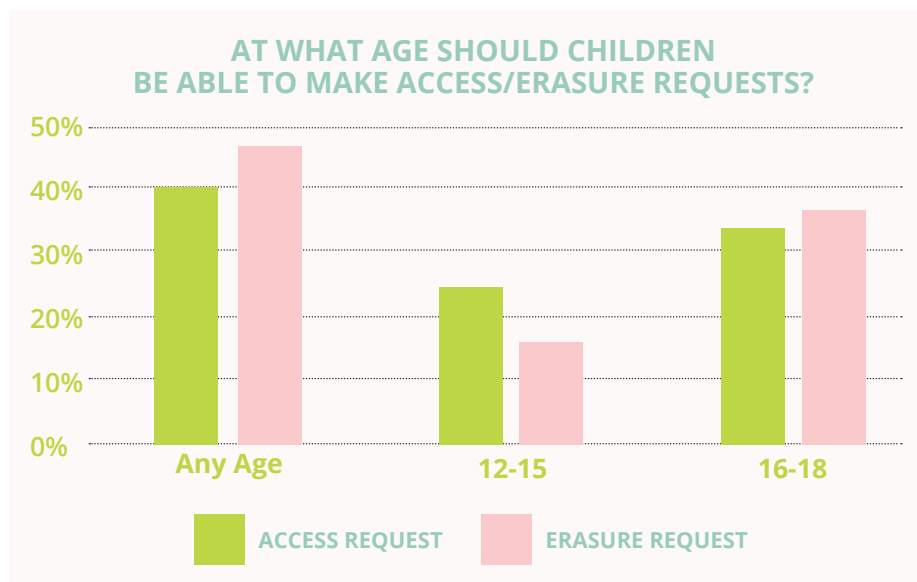
SHOULD TWO SEPARATE SETS OF TRANSPARENCY INFORMATION BE PROVIDED THAT ARE EACH TAILORED ACCORDING TO THE RELEVANT AUDIENCE?



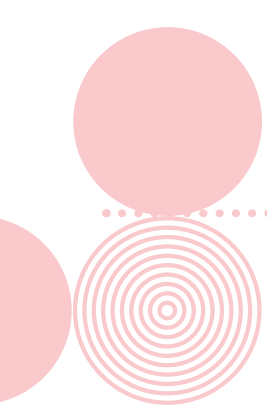
Those opposed to the suggestion of having two sets of privacy notices tended to highlight the legal uncertainty that may arise from having two sets of transparency notices, or argued that it should be possible to provide a single notice that is suitable for both adults and children, for example through the use of layered information notices incorporating things such as audio-visual content, just-in-time notifications, and graphics. Others argued that content parity should be the objective for all organisations but that, nevertheless, two sets of privacy notices may be necessary in certain circumstances. At least one participating organisation stated that they would be publishing a child-friendly version of their privacy notice over the next year.

Exercise of data protection rights

Respondents were particularly interested in the consultation questions relating to the age or the circumstances in which children should be able to exercise their own data protection rights. The following chart compares the answers given in response to questions 3 and 6 of the consultation document, which concerned the age at which children should be able to make access and erasure requests, respectively. Although many respondents gave the same answer to both questions (and often wrote “as above” or “see above” in their submissions), there were some interesting variations in the answers given:



The most popular answer to both questions was that children should be able to make these requests at any age. However, many who gave this answer also said that such requests should be made by children with varying levels of cooperation and dialogue with their parents or guardians. Interestingly, more submissions were in favour of children being able to make *erasure* requests at any age than children being able to make *access* requests at any age. In



other words, they considered these rights to be two separate issues as opposed to viewing them as part of the same overarching right to exercise one's data protection rights. Respondents seemed to have a more paternalistic view when it came to allowing children to submit access requests at any age, yet more of an enfranchising view in respect of erasure requests.

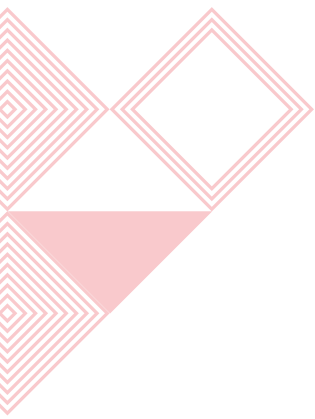
Those in favour of granting access requests at any age often drew attention to the fact that children may need help from parents in making sure that their access request is complied with and in examining and understanding the personal data returned to them. Responses in favour of children being able to make erasure requests at any age were more often couched in terms of respecting children's fundamental rights, particularly in circumstances where a child has previously given consent to processing without being fully aware of the risks and now wants to have their personal data deleted.

Alternatives to age-based factors

The majority of respondents were keen to point out that age alone was a far from perfect metric in assessing the capability of a child to exercise his or her data protection rights, and called for a wide range of additional factors to be taken into consideration. Many respondents prioritised the level of cognitive development of the child, and pointed out that there can be considerable variation in the intellectual and emotional development in children of the same age, particularly in early adolescence. Some respondents stated that a child's level of education, participation in extracurricular activities, and disciplinary records if any, could also be relevant criteria. Other respondents were more concerned by the vulnerability of the child, his or her family situation and the circumstances under which the erasure or access request is issued. Some organisations also emphasised that extra consideration should be given to children who are particularly vulnerable, for example children with disabilities or emancipated minors.

Parental involvement

Regarding parental involvement, most submissions agreed that there should be limits on a parent or guardian's ability to exercise their child's data protection rights, particularly for children approaching or at the age of digital consent (i.e. 16 years old). Most felt that parents should be able to exercise these rights on behalf of young children, but that adolescents should have a certain degree of involvement or control. Several submissions emphasised that



these rights belong to the child and not the parent, and therefore it is important that children are able to assert the rights themselves, especially in situations where they are in disagreement with their parents.

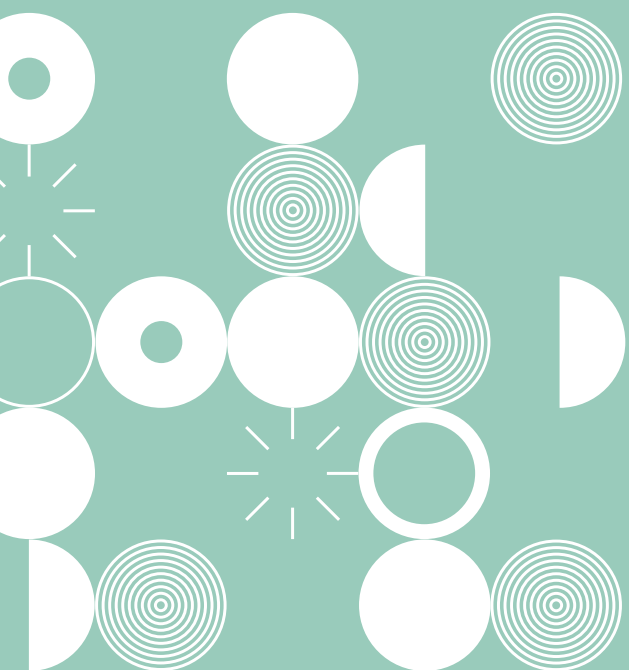
Respondents tended to agree that, from the age of 16 onwards, children should be in the driver's seat. They should be encouraged to seek the support and advice of their parents when exercising their data protection rights, but they should not be *obliged* to do so. Several respondents felt that parents should still have the power to intervene in exceptional circumstances in order to protect the vital interests of the child, such as in cases of online harassment or cyberbullying, or where children have put themselves in danger. Others were wary of the risk of coercive or estranged parents using such powers to harm their children.

Some submissions pointed to existing guidance available under the Freedom of Information (FOI) Act 2014 in Ireland produced by the Office of the Information Commissioner on processing FOI requests from a parent or guardian seeking to access a child's records, stating that this may be an appropriate reference when it comes to dealing with requests from parents or guardians to exercise a child's data protection rights on their behalf. As set out in one submission, these FOI guidance notes include a number of factors that can be considered when a request is received from a parent or guardian and the record relates to a child, for example:

- The age of the child – the closer the child is to the age of 16/18, the more weight should be placed on their view as to whether records should be released;
- Whether the records are held in the child's own name
- The nature of the records – the sensitivity of the information; the basis upon which it is shared by the child, etc.
- The nature of the relationship between the child and the parent/guardian – e.g. are there any court orders relating to parental access or responsibility that may apply, etc.?
- Whether the child would consent to the release to the parent and any views or opinions expressed by the child – e.g. is there any duty of confidence owed to the child?
- Whether granting access to the record would damage the child in any way; and
- Whether granting access to the record serves the best interests of the child.

The submissions which were in favour of following the FOI approach took the position that this established FOI regime provides a suitable template for handling requests made by a parent/guardian to exercise their child's data protection rights on their behalf.





Safeguards


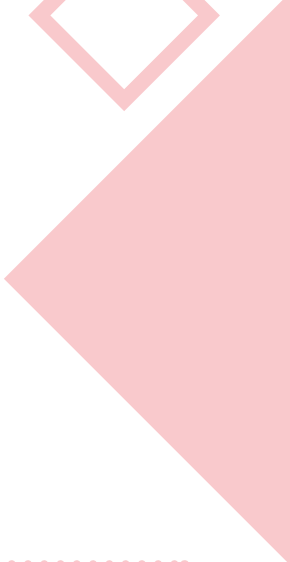


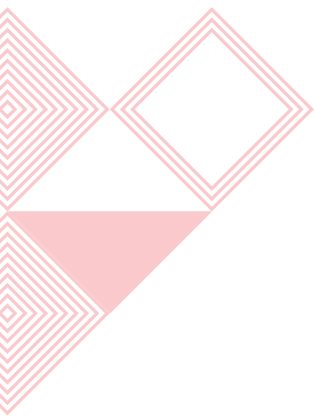
II. Safeguards

Age verification methods

In Ireland, data controllers who are online service providers cannot rely on consent given by children below the age of 16 (the “age of digital consent”) to process their personal data. Instead, parental consent must be given. In other words, consent must be given by the person who holds parental responsibility for the child. However, the GDPR requires that the online service provider must make “reasonable efforts” to verify that consent is given by the holder of parental responsibility “taking into consideration available technology”.

On the question of what methods should be used to verify that a child has reached the age of digital consent (where consent is the legal basis for processing a child’s personal data), a range of solutions were suggested by stakeholders, for example:

- Implementation of age gates, in which children can either freely enter the day/month/year of birth, or use a drop-down menu that includes ages that are both under and over the age of digital consent. One submission suggested implementing further technical measures to prevent users from “back buttoning” if they enter an age that is below the age of digital consent.
 - Request users to provide official ID that is immediately deleted – however, many of those who suggested this solution admitted that it would be hard to justify this request given the principle of data minimisation and the resulting commitment to collect only the minimum amount of data necessary to achieve the purposes of their processing activities.
 - Co-signed parent/child consent forms
 - Two-step verification such as emails, text messages or phone calls to parents or guardians
 - Use of secure third-party verification services
 - Device-level verification – one submission provided a specific example in the context of mobile phone apps. They stated that many apps that a child may download to their mobile device involve a third party, namely a mobile carrier or the platform’s app store. These apps require the customer to have an account with the mobile carrier or app store. The submission took the view that there are opportunities for these third-party businesses to maintain an age authentication feature tied to the customer’s account. When a child wants to download an app that processes personal data, the third party account can be used to verify age.
 - A “knowledge check” method, requesting information less likely to be known to people under 16
- 
- 

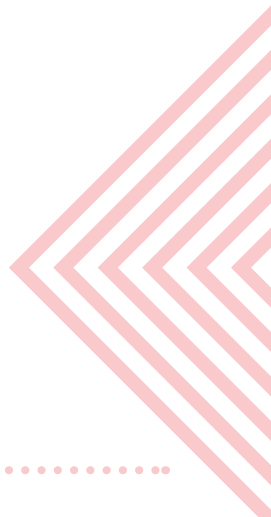


Several respondents pointed out that the most appropriate approach to age verification would depend on the context, such as the service being provided and the sensitivity of the personal data being processed. Some organisations also suggested that age verification may not be the answer, with one stakeholder 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 pop-up 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.

Another question put to stakeholders was "What methods can online service providers use to ensure that the person providing consent is actually the holder of parental responsibility over the child?" Several submissions expressed scepticism that this was achievable in a way that is not overly intrusive under the GDPR. 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, while another suggested requesting the electronic signatures of parents to discourage potential bad actors. Many submissions called for a proportionate risk-based approach, whereby proof of ID could be requested from parents for sensitive data and/or high-risk processing, but for lower-risk processing, they suggested that email or text verification might be sufficient. 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.

Other organisations echoed the methods used by the Federal Trade Commission (FTC) in the US under the Children's Online Privacy Protection Act, or "COPPA" as it's known, including validation through calling a toll-free number staffed by trained personnel, answering a series of knowledge-based challenge questions that would be difficult for someone other than a parent to answer, or through a micro-payment on a credit card. This last suggestion, however, was also flagged by some stakeholders as a potentially exclusionary solution, as they believed it could disadvantage users who do not have access to a credit card.

As regards what would constitute a "reasonable effort" by data controllers to verify the identity of a child's parent or guardian, most respondents believed that this would depend on several factors including the risks associated with the processing and the vulnerability of the child, and that if the risk is high, then the efforts by the organisation to verify the holder of parental responsibility should reflect this approach.






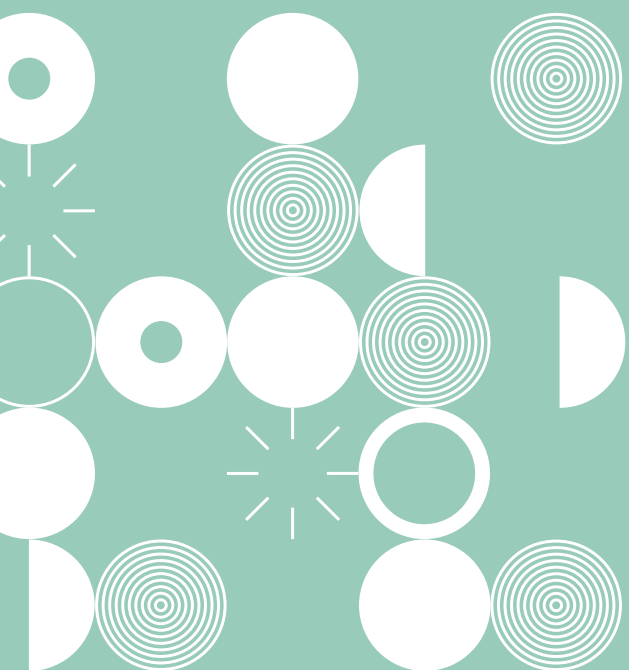
Withdrawing access to online services offered pre-GDPR to children under the age of digital consent

One of the consultation questions asked respondents to consider the scenario where a child between the ages of 13-15 has given consent prior to 25 May 2018 to an information society service to process their personal data in order to use their service. With the entry into force of the GDPR, if the child is still under 16 and consent is still the lawful basis for the processing, should he or she be locked out of the service until they turn 16? The most common answer to this question was that a child should not be locked out of services to which they signed up legally pre-GDPR. Those who were in favour of shutting off access to this service tended to be charities and children's rights organisations, who argued that the law is clear that it is unlawful for organisations to process the personal data of children under the age of digital consent without parental consent. However, several submissions argued that it should be possible to prevent this problem by allowing affected data controllers to either adapt their services accordingly or to prompt children under 16 to provide retroactive parental consent. Submissions from the private sector tended to be against this proposal, with one arguing that such an abrupt shift would be harmful to children who have come to rely on the service (e.g. for study purposes). It was also argued that it would be unfair to apply the GDPR retroactively to processing that was legal before 25 May 2018. Others pointed out that such a proposal would be difficult to enforce in practice.

Online service providers and different national ages of digital consent in the EU (Article 8 GDPR)

When asked how data controllers should comply with differing ages of digital consent across the EU, the most frequent suggestion was that online service providers should make sure that they have the appropriate technology and/or infrastructure in place to meet the requirements in each country where they offer their services. Examples of this included providing drop-down boxes on their homepage allowing children to select their country of residence, monitoring users' IP addresses, employing age gates or setting up multiple website domains. Other suggestions included identifying and applying the relevant law in each country, or simply ignoring the varying age thresholds and instead applying the highest age threshold across the EU due to the complexity involved in implementing varying thresholds. One submission called for "a relevant organisation such as the European Data Protection Board" to be the official source for providing a centralised, publicly available resource listing the ages of digital consent per Member State in an easy-to-read format and explaining the derogations in relation to the "age of digital consent" made by EU Member States.





Profiling and marketing activities concerning children

(Articles 21-22 GDPR)



III. Profiling and marketing activities concerning children (Articles 21-22 GDPR)

The GDPR does not impose an outright prohibition on organisations marketing or advertising to children, but it does say that they should apply specific protections for children when marketing to them or creating user profiles. Additionally, collective guidance issued by the EU's data protection authorities (European Data Protection Board ("EDPB")) advises that, because children are more vulnerable, organisations should, in general, refrain from creating individual profiles on children for marketing purposes. All individuals (including children) have the right to object at any time to their data being processed for direct marketing purposes. When asked what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing against the interests and rights of a child who is being marketed to, a number of submissions proposed factors such as:

- the level of cognitive development and social awareness of the child
- the degree of risk of harm associated with type of product or service being offered/marketed to the child
- the intrusiveness or sensitivity of the data being processed in order to profile the child
- the child's ability to process the information appropriately
- the capacity of the child to understand that they have the right to object

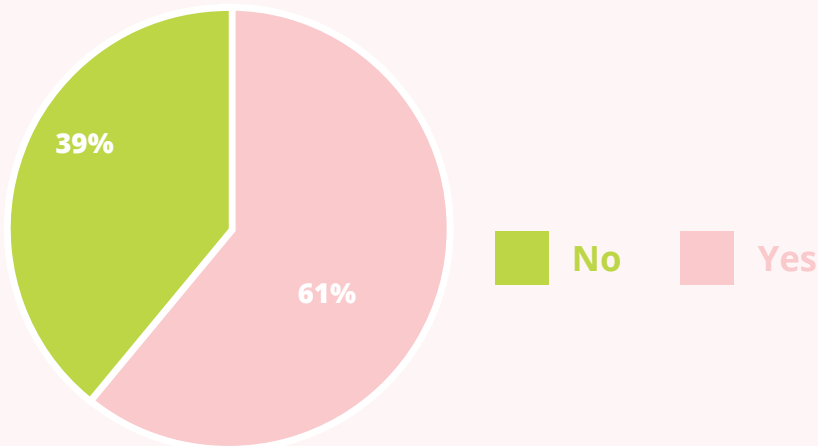
Most submissions argued that more weight should be given to the rights and interests of the child in any balancing test being undertaken, and that a child's lack of understanding should not be exploited for commercial gain. It was also strongly felt that the legitimate interests of the data controller should only have weight in a limited set of circumstances, for example where processing personal data is required to ensure that ads are shown to a human as opposed to a bot, and that where a data controller may have a legitimate interest, the onus is firmly on them to demonstrate this.

Profiling children for marketing purposes

We also asked stakeholders whether they thought organisations should be banned from profiling children for marketing purposes. Of the submissions that came down firmly on one side or the other, 61% were in favour of banning organisations from profiling children, while 39% disagreed with the idea of a ban (primarily technology companies). Those who were opposed tended to argue that Article 22 of the GDPR does not explicitly prohibit solely automated decision-making (including profiling) where

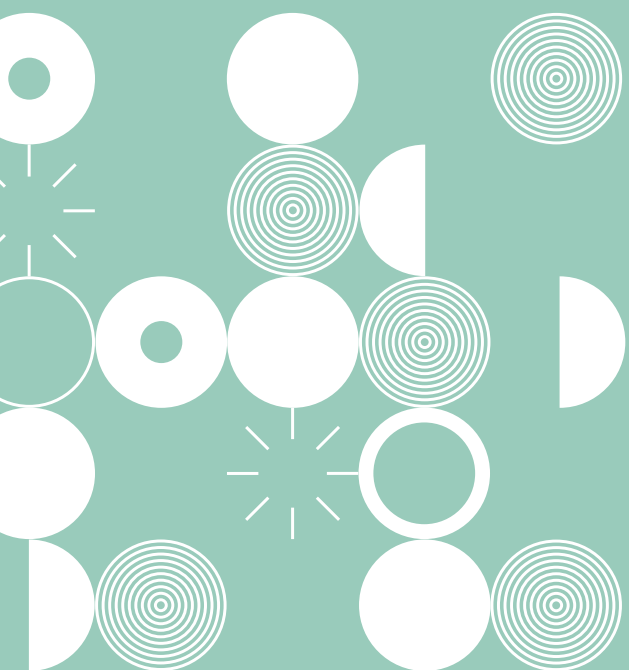
children are involved if such processing does not have a legal or similarly significant effect. They believed that there should be no issue in profiling children for marketing purposes provided that organisations have strong safeguards in place, and that parents should be allowed to decide whether they want their children to receive marketing communications or not.

SHOULD ORGANISATIONS BE PROHIBITED FROM PROFILING CHILDREN FOR MARKETING PURPOSES?



Those who were against the profiling of children for marketing purposes pointed out that parental consent was not much of a safeguard since many adults – let alone children – are unaware of the quantity and quality of personal data that can be disclosed through commonplace online activities, and that this is particularly troubling where children are concerned due to their vulnerability and susceptibility to online advertising. One submission stated that it has been found in many instances that children do not intuitively regard their social online interactions as being subjected to ongoing monitoring despite research to indicate their increasing awareness of such commercial practices, and that there should be no justification to allow the profiling of children of any age since such commercial practices tend to have negative effects, primarily due to a lack of experience and maturity.

Another submission expressed concern at ‘advergames’- in which online adverts are combined with free playable games – arguing that these take advantage of children who may be too inexperienced to realise that they are being targeted with advertising and that they are sharing their personal data through playing these games. Others expressed concern that exposing children and young people to targeted advertising would affect their cognitive and psychological development. One submission reported that they had consulted with children directly on this issue and that some of these children had expressed strong opposition to organisations being allowed to profile them.



Data protection by design and by default (Article 25 GDPR)

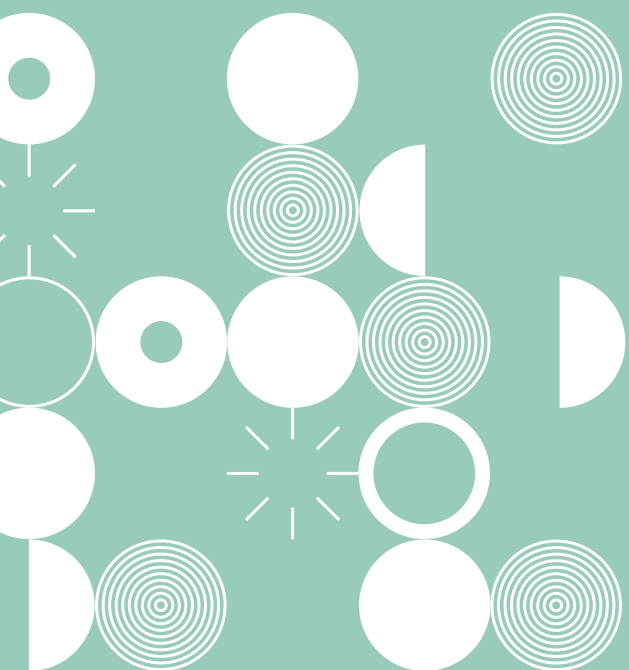
IV. Data protection by design and by default (Article 25 GDPR)

The GDPR imposes a new obligation of data protection by design and by default on organisations who process personal data. This means that data protection and privacy protection should be built into 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 (rather than the user having to activate them). These obligations are particularly relevant considerations for organisations whose products or services are used by or offered to children. When asked how best to incorporate the principles of data protection by design and default into services and products used by children, participants gave a wide range of answers, covering both technical and organisational measures. The following are among some of the suggestions put forward by respondents:

- Implement procedures that ensure data minimisation: The vast majority of submissions recommended retaining children's personal data for the shortest amount of time possible, and implementing strict retention periods. A number of stakeholders suggested that data controllers should anonymise, pseudonymise and even redact all categories of personal data of children.
- 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

Built-in privacy settings for children

The DPC also posed the question of whether products/services that are used by or offered to children should have built-in default privacy settings that vary according to the age and evolving capacities of a child. The majority of submissions were in favour of the principle of having higher default privacy settings for children. However, some expressed scepticism that age was the best metric for determining this, stating for example that children aged 6 and 14 are the same in the eyes of the law and should be treated the same in terms of privacy, while others warned that this proposal would be difficult to implement in practice or that it might clash with the principle of data minimisation. As a result, most submissions were in favour of higher default privacy settings for all children across the board, regardless of age. Suggestions were made that children could opt for less strict privacy settings as they got older and if, for example, a child decided to opt for more public settings, there should be an option to involve parental consent as a possible two-step verification process, or warnings/just-in-time notifications could be provided to children in an accessible format, such as graphics or cartoon characters, pointing out the risks that the child is leaving themselves open to, rather than a text-heavy warning notification.



General



V. General

When asked if there were any other issues which respondents would like to raise within the framework of this consultation, respondents provided a wide range of answers. Some gave constructive feedback in terms of expanding and developing the parameters of the consultation. For example, some submissions suggested that more attention be paid to safeguarding the rights of children with disabilities, particularly since they can be disproportionately reliant on online services. Others wanted more opportunities to share perspectives and best practices on protecting children's personal data with other stakeholders. For example, one submission stated that it would value input and guidance from specialised civil society groups, and particularly children's rights advocates, on the elements to consider when striking that balance in the way that best protects children's interests. The National Advisory Council for Online Safety (NACOS) was suggested as potentially being a suitable forum to inform this exercise.

One submission shared concerns regarding what they perceive to be excessive reliance by organisations on legitimate interest as a legal basis for processing personal data, while other stakeholders highlighted the importance of educating parents about the risks of sharing their children's personal data online and the implications this may have on their children's data protection rights. One organisation called on the DPC to issue guidance on instances where the GDPR may interact with child protection legislation, and separately on whether the new age of digital consent will affect the ability of children and young people to give their own consent to participate in research.



Conclusion

The DPC received a large number of submissions from organisations and individuals spanning many sectors of society as part of this consultation. Each submission demonstrated a significant degree of engagement with the issues that were raised in the questions posed by the DPC. This, combined with the wide spread of views shared between submissions received from private, public and civil society organisations, means that this stream of the consultation is a valuable resource to the DPC as it drafts guidance for individuals and organisations going forward. The most striking result at this early stage in the DPC's analysis of these submissions is the manner in which the various categories of participants in the consultation align and diverge on many issues related to protecting children's personal data. As discussed above, there was a significant level of divergence between the private and non-private sector participants on several issues in terms of how best to protect children's data online, including on whether or not

to offer separate privacy notices for adults and children, whether children should be shut out of services until they turn 16 in certain circumstances, and whether profiling of children for marketing purposes should be allowed.

At the same time, some questions appeared to unite participants across sectoral lines, for example on the best strategies for conveying transparency information to minors, and on issues relating to the tension between parental involvement and children's autonomy.

The DPC is very grateful to all those individuals and organisations who took the time to participate in this consultation. Further and more in-depth analysis of the submissions will no doubt continue to inform the DPC's focus on the area of children's data protection issues as it moves towards the next phase of its work in preparing practical guidance for children and organisations alike.



