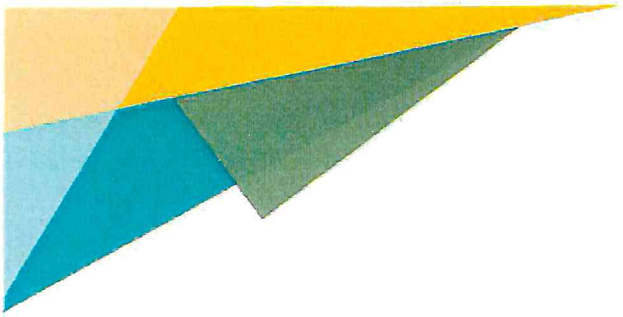

CASTLEBRIDGE

Changing how people think about information

Consultation on Data Protection Rights of Children

April 2019

Contents

About Castlebridge

Founded in 2009, Castlebridge has been at the forefront of Data Governance and Data Privacy consultancy and training in Ireland for almost a decade. Our team are internationally recognised thought leaders in the fields of Information Governance, Data Privacy and Information Ethics. Our founder has been an award-winning industry expert for over twenty years.

Castlebridge takes a pragmatic and practical approach to client engagements, with a strong ethos of telling the client what they *need* to hear, providing objective, evidence-based assessments, applying proven and reliable methodologies, and delivering market leading expertise through our core team and our network of industry partners around the world.

We are a vendor neutral, research-driven consultancy focussed on giving clients the tools they need to change how people think about information, and ensuring that your internal teams can trust the quality and provenance of the data they use to do their jobs, and your end customers can trust that your organisation will handle the data that describes them ethically and in compliance with relevant laws and best practices.

Our clients include leading public and private sector organisations in Ireland, the UK, the US, and Europe.

Children as Data Subjects

In this section we set out our submissions in respect of the first 16 questions.

Transparency and Right to Be Informed

Question 1

What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?

The answer to this question is contingent on the age groups being targeted or addressed by the Data Controller. Consideration should be given to factors such as:

1) Literacy levels
2) Level of understanding and comprehension
3) Attention span
4) Level of psychological development, including whether the average child would have comprehension of abstract concepts such as risk.

Attention should be paid to how well the mode of delivery and format fits with the level of cognitive development that a child in the target age group would demonstrate. The classic reference here is to the work of Piaget and it is important that the explanation of concepts take in to account the often concrete and literal way younger children in particular can see and interpret the world.

Based on the personal experiences of our team explaining processing activities of online applications or games to young children, it would also be appropriate for information to be provided to *adults* to help them explain to children the meaning of information that is being provided to them in a way that is appropriate *to that particular child*.

The "traditional" approach to privacy statements is largely legalistic in its approach and emphasis and, as studies have shown, are not suited to the needs of younger data subjects.

Rather than advising on a specific range of approaches, Castlebridge would instead advise that organisations engaging in the processing of data of children engage advisory support and guidance from organisations with experience of children's education to ensure that they design their child-focussed interactions in an appropriate manner using appropriate media, design, and language.

Examples of approaches that could be used to communicate and convey information to children could include:

1) Use of short videos or animations to provide "in context" explanations of processing purposes and uses of data
2) Use of visual cues or explanations that are anchored in more readily familiar concepts
3) Appropriately drafted text that is aimed at the relevant reading age
4) Gamification of the communication of information so that the concepts are communicated in a memorable manner.

Organisations might want to present information in a more immediate context to children to remind them of what is going to be done with information at that point in the game or online service.

This will, of course, require consideration to be given by organisations who are targeting services at children to how they will explain their processing in a manner that will enable adults to understand and explain to children the processing activities and purposes of information.

This empowerment of parents and guardians to explain should be seen as an important consideration from two perspectives.

Children need to be able to ask parents so they can allay fears

Firstly, it is essential that adults are able to explain to children what is actually meant by the concepts that are presented to them in the "kid-friendly" version of the privacy statement. It is a key component of the Stay Safe programme in primary schools that children should talk to adults about things that upset them in an on-line environment. This should extend to the child being able to seek clarification from their parents about things that might be bothering them or about which they are curious in the context of how their information is used by organisations.

However, this means that parents must have access to appropriate knowledge to help answer questions in an informed manner themselves so that children feel they can actually get meaningful answers from their parents.

The personal experience of our Managing Director in this context is, we feel, an important reference. [redacted] has a 9-year old child[1]. Since his child began to go online and began to be asked for information about them by organisations (schools, activity and sports groups, etc.) he has encouraged his child to ask questions and feel

---

[1] [redacted] *will be making an independent submission in Strand 2 of the consultation. Please note that this topic was not raised in the school and was something that was requested by the child.* [redacted] *is grateful to the Castlebridge team who helped answer questions and encouraged the development of this submission.*

they are able to make choices. He has discouraged the sharing of images on social media however.

For a while this became conflated in the mind of the child with unknown "bad guys" who might do nefarious things if they had access to the child's image or other data. This is despite [redacted] having approached discussions around online privacy and data privacy with his child in collaboration with his wife, who is a qualified teacher.

While, as a data privacy professional of over 22 years' experience, [redacted] might indeed feel that this is the case (for "bad guy" insert "venture capital backed advertising network"), it is clear that even with specialist knowledge and experience reading and interpreting privacy statements and analysing the operation of data processing applications and experience in framing concepts to teach them to children, this is not something that can be easily done.

As most parents will not have the benefit of half a life time's specialist experience, Data Controllers should provide explanatory collateral.

For persons with parental responsibility to give informed consent, they need to be informed

For consent under Article 8 to be valid, there are two key tests to pass in our view:

1) Did the child understand what they were agreeing to, even if they had to ask their parent/guardian to help explain it?
2) Did the parent/guardian understand what they were agreeing to, and were they able to explain it if asked?

For this reason, we are of the opinion that "parent friendly" explanatory supporting material should be provided to help parents make informed and unambiguous choices about the processing of a child's data.

Summary of Answer

1) Privacy by Design/Default requires the level of literacy, comprehension, attention, and other factors relative to a child to be considered at all times. Therefore, there is no "one-size-fits-all" recipe for communicating these concepts to children.
2) Parents need to be empowered and supported to answer questions and explain to their children in terms their children will understand and in a way that will not scare or disturb children. Data Controllers need to address this.
3) Without parents having the means to inform themselves and answer questions from their children, it may be difficult to argue that there is adequately informed consent from either the child or the parent under Article 8.

Question 2

What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separate sets of transparency information be provided that are each tailored according to the relevant audience?

The answer to this question is found in the text of GDPR itself. Article 12(1) sets out a number of key considerations for the drafting of privacy notices and the communication of information to data subjects.

The communication must be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed *specifically to a child*" (our emphasis).

In the context of the points we raised in relation to question 1, we would argue that Article 12 requires different treatment to be applied to information being provided to children. The only exception to this we can envisage is where the privacy statement is written *in its entirety* in language that is readily understood by a child without the need for further explanation and where all the processing activities of the organisation can be encapsulated in that one child-friendly version.

However, given the need we see for parents/guardians to be empowered and supported in answering questions from their children about what is meant by terms or concepts in a privacy statement, we would be of the view that an "adult appropriate" version of the privacy statement that references back to the child-focussed version is a key enabler of informed consent and informed choices by both children and parents.

In the context of organisations that offer different categories of products or services to children and adults, we would answer this question with the simple point that many of the great works of literature have "child friendly" versions where the language is simplified while retaining the core essence of the story. That this has evolved as an approach to teaching literature and literacy to children should give pause for consideration as to whether different treatments of the same core text should be considered when seeking to communicate important concepts to younger readers.

Summary of Answer

Yes. Different audiences require different presentations of the same information in an appropriate and intelligible manner.

Question 3

At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?

There should be no age barrier on a child making an access request to an organisation. Simply put, the right of access is the price that is paid by an organisation for having data about identifiable persons. The right of access is a fundamental right under Article 8 of the Charter of Fundamental Rights. Age should not be a factor.

Our managing director's 9-year-old has, on their own, already successfully submitted Subject Access Requests to a number of Data Controllers (including Santa Claus, and a crèche). While this particular child may be particularly precocious in their knowledge of their data protection rights, it is clear that an informed child is capable of making a request to exercise their right of access, particularly as the required form of request is no more complicated than "Please give me a copy of my data".

However, even fundamental rights can be restricted or curtailed in certain circumstances. Factors such as the level of comprehension of the child, their level of cognitive development, and the potential for distress to be caused to a child if the information provided is not properly explained in terms that they can understand, as required under Article 12.

Therefore, the question should not be at what age a child should be able to make an access request, but rather what form should the response to that request take to ensure that the child's rights are upheld in an appropriate, balanced, and effective manner.

Consideration should be given to

- how SAR processes are defined so that they are accessible to children, which will in turn improve their accessibility to adults;
- how information is presented in response to an SAR from a child so it is executed in an age appropriate manner;
- how appropriate security measures can be applied to the execution of the SAR response to protect the interests of the child. For example, in the case of online services, notifying the parent who approved the consent and only responding to the SAR when that person confirms the request.
- How information is formatted and presented to children (again, this would benefit adult data subjects as well, particularly those with cognitive impairment or learning difficulties.)

Summary of Answer

The right of access is a fundamental right under Article 8 of the Charter. Age is not a barrier to the exercise of this right, nor should it be.

However, factors relating to the individual, which may be a function of their age but could be related to other factors, will require consideration to be given to how SARs would be executed in this context to ensure an appropriate balancing of rights against other considerations such as the security of the data subject or ensuring they are not exposed to upsetting or confusing material.

The key test is one of comprehension and cognitive ability rather than chronological age and Data Controllers should design for this anyway in the context of their obligations under Article 12.

Question 4

In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?

The ability to make a subject access request on behalf of a child and receive a copy of a child's personal data must take into account the role of guardianship a parent or other guardian has, and the capacity a child has to consent on their own. The voice of the child should be considered, as the primary question here is the child's right to their own data as a data subject, not a parent's right to their children's data. Once a person has reached the age of majority or is legally emancipated, a parent should not be able to obtain their data without their consent. While a guardian's ability to access a child's personal data may be essential to enable a child's rights and freedoms and to ensure a parent or guardian can act in the interests of their child, the evolving capacities of the child, their right to free development of their personality, and rights to freedom of expression and ability to seek information should be taken into consideration.

Data controllers and processors must consider that in some cases, providing data about a child to a parent who is not a guardian could put that child at risk. Our head of Training and Research observed a situation where differing schools' approaches to student privacy resulted in one school providing information to an estranged and abusive parent that enabled parental kidnapping of two children, while the more stringent privacy policy of their older sibling's school preserved their safety.

While it may be overly burdensome for a data controller to be able to determine the guardianship status of a parent, a reasonable compromise may be to supply subject access request responses to the child at the address of primary residence of the child.

As children grow older, increasing in cognitive development, maturity, and independence, their rights and freedoms to support their dignity in self-exploration and development of personality will include an increased emphasis on a right to privacy which may indeed include the need to keep aspects of their development private from their parents. For instance, a child in an extremely socially conservative family environment may require privacy from their parents in order to obtain information regarding their sexual development or sexual or gender identity in a safe and supportive environment.

The milestones already defined in law for the age of digital consent may be a guideline for comparison here. We would suggest that with due consideration to protection of the child, 13 as the lower possible age suggested as a derogation for the age of digital consent in GDPR and a common milestone for adolescence may be a reasonable age to require a parental Subject Access Request to be made jointly with the child, at least when involving information that might reveal communications or sensitive content.

Consideration should be given to:

- The evolving capacities and increasing autonomy of a child as they develop in maturity
- The increasing importance of privacy to psychological and social development
- The "edge case" scenarios where providing data to a parent may not be to the benefit of a child
- The special requirements that children with physical or mental disabilities may need
- The special care that may need to be taken to protect children who are discovering aspects of their personality, gender identity, or sexuality, and/or who do not live in a supportive family environment.

Due consideration must be paid to non-conventional family units. How far data controllers should go to take non-conventional family units into account is a risk-based decision.

Summary of answer

The right of access under GDPR is the right of the data subject not a parental right, and parental access to children's data should be provided where necessary to preserve the rights and freedoms of the child. Parental guardianship should be taken into account before releasing data.

Parental access to children's data should be proportionate to the cognitive development and increasing independence of children, to preserve the personality rights of children and adolescent minors.

Non-conventional family units must be taken into consideration when devising policies. A risk-based approach must be taken.

We would suggest 13 as an age where a parental subject access request on behalf of a child should be taken jointly with the child.

Question 5

How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?

A person is regarded as having personal data from the day they are born. This is reflected in the definition of personal data in Article 4 GDPR. The question is therefore one which involves assessing the ability of a child to understand in a clear way their right to privacy in order to control access to it. There are different aspects of a child's life which may attract questions of privacy and in certain scenarios a guardians right to access may overlap or trump that of the child.

It is important to understand these issues in terms of guardianship rather than parentage as it is the guardian who has the rights in relation to a child under Family Law Legislation, whereas a parent may in certain instances have their right to guardianship revoked. In that instance, verification of guardianship is of importance, and clear guidelines for verification should be given in order to avert the possibility of a data breach.

Summary of answer

While there will always be an issue in regard special cases, for clarity and direction it may be of use to have a base line which to follow in more standard access requests. It is suggested that there are two separate strands to this:

A Guardian should have access to the personal data of a child up until the age of 13. The Guardian must show *need* for accessing the personal data of the child after this age. In certain scenarios the Data Controller may feel the need to seek out the voice of the child from an earlier age. This is to be done on a case by case basis.

The second strand relates to a child's right to access data from the age of 13, and in certain cases earlier, with the controller having a right to object until that child turns 18 in certain cases.

The legal reasoning

Data Privacy Law

Rights of the child to make a data subject access request on their own behalf. This may be a separate process. Section 29 of the DPA 2018 outlines that

"For the purposes of the application of the Data Protection Regulation in the State, a reference to "child" in the Regulation shall be taken to be a reference to a person under the age of 18 years"

The underlined phrase is problematic as it is open to suggestion that only a person 18 years or older may invoke their rights under the Act. This is in direct contrast with Section 31 of the DPA 2018 which indicates that a 16 year old may engage with 'information society services'.

Recital 38 of GDPR is instructive as it states that children need extra protection in relation to their personal data, as they may not be aware of the risks, consequences and safeguards in relation to 'processing' personal data. The risk foreseen therefore is that of giving your data away at a young age, rather than seeing what is there already at that same age. Article 8 GDPR clearly outlines that Regulations may be made by individual countries in relation to information society services with regard access by age, from 13 years old upwards. Therefore a baseline of 13 is suggested in relation to a child accessing their personal data, but only with appropriate safeguards in place.

Specific circumstances in other legal spheres

The age of criminal responsibility, with reference to the Childrens Act 2001 as amended, is 12 years and 10 years for serious offences. It is clear therefore that society has deemed that children do have capacity in certain instances before the courts and further it must be noted that these ages have been set and based on years of extensive and varied case law, something that the law of data privacy has not had in the same way.

Once again Family Law practice may be referred to, where the 'voice of the child' is regularly invoked in family disputes by a Judge hearing contentious cases. In this scenario there is considerable leeway once a Judge interacts with the child the extent to which the child may have capacity to understand and give direction as to their wishes in the context of proceedings before the court.

Therefore, it is clear that society has given weight to the mens rea of children below the age of 13 and that it is important that there be provision for this to be explored in the case of access to the personal data of children aged 10 and above. In particular cases it may be that the voice of the child should be heard in a similar manner as that which is done in Family Law proceedings.

Some examples

Psychological file; The reason for denial of access to a child's file may be the same for both guardian and child. If it is not in the interests of the child for either guardian or child to have access, then it is incumbent on the data controller to deny access on this basis.

Teachers notes; while it is unlikely to be popular, there is a strong likihood that all data relating to the child may be accessed by the child during the period of their attendance at school in the normal fashion. This may not apply when relating to issues arising from psychological profile as are outlined above. This is not the area of expertise of a teacher in most situations therefore it is the relevant professionals who must outline clearly to the teacher what information may not be divulged to the child by this means at the time of passing to the teacher and appropriate training should be given to teachers in relation to same also.

Online activity and sexual identity; It is likely that there is cause for conflict at the age of maturation in relation to certain issues regarding the oncoming adolescence. Issues such as sexuality, gender identity may be regarded as being very private at the developmental stage. Should say a guardian from a particular background seek access to online activity of a child in their care who may be in the first stages of identifying as gay a friction develops between the rights of the guardian and that of the child. It is clear that in such a scenario, any social issues such as these should not be accessed by the guardian without good reason. It may be that access to pornography is in the interests of the guardian, however if it goes in some way to determine a hidden sexual preference it may be that the rights of the child over-ride this. It is clear that in this instance a reference may be made to another party to determine what is allowable.

If you hold back the data from a guardian on the basis that it *would* determine sexual preference, this act in itself could be interpreted as a confirmation of sexual preference by the guardian. Therefore, all personal data related to sexuality must be only given to a guardian on the basis that they have a good reason to know. I.e. if there is a

documented reason to believe that a child has developed an addiction to pornography which is having a detrimental effect on the child. The child must be engaged with this process and given an option to object.

Question 6

At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration?

Please note 4&5 above, the key factor is whether the child will understand the consequences of the erasure request and is there an alternative mechanism that could be applied in certain cases– restriction etc.

Question 7

In what circumstances should a parent be able to make an erasure request on behalf of their child and have their child's personal data erased? Is there an upper age limit after which a parent should not be able to make an erasure request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an erasure request?

See above in relation to upper age limits and the joint agency of guardian and child. There will undoubtedly be situations where a guardian may unilaterally seek the erasure of personal data relating to a child. This is clearest where, the child does not have requisite capacity to object, the child has been the victim of mistake/misrepresentation, the non-erasure of personal data would mean the continued or future harm to the child.

Once again alternatives to erasure must be considered in this context, i.e. restriction.

.

Question 8

If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could/should be used to verify that a child is 16 or over in order that the child is granted access to the online service without the need for parental consent?

This will change with the state of the art and the service provided and will rely entirely on the types of information available to the data controller. The requirement for age verification must be balanced against the invasiveness of the method used to verify age and should not require disproportionate processing of personal data in order to verify age.

A less invasive method is a knowledge check, with information less likely to be known to people under 16. While not wholly reliable, it does not require extra processing of personal data and is more reliable than simply the subject to state their year of birth.

Question 9a

What methods could/should online service providers use to ensure that the person providing consent in these circumstances is actually the holder of parental responsibility over the child?

Please see 9b

Question 9b

What constitutes a "reasonable effort" made by organisations to verify such consent is being given by a person who is actually the holder of parental responsibility over the child? How should "reasonable efforts" be measured in this regard?

The dangers in relation to verification are highlighted most clearly in family law situations. Guardianship is what determines right to access to a childs personal data. Most parents are guardians however guardianship may be revoked. Therefore there is a gap that could be exploited by a parent who is not a guardian in accessing crucial personal data of children. In this context it must be understood that guardianship is often only revoked in very serious circumstances which require a high bar of proof.

As with most issues clarity may be provided at the point of capture, that any guardians be listed when data is first provided to the controller. In this instance if a data subject is recorded as having guardianship, then once an access request arrives this can be verified against the record of guardianship and the ID of the guardian making the request.

In cases where more serious data may be subject of the request, if there is more than one guardian listed that it be verified with the second guardian that the first is in fact still a guardian of the child.

If there are serious concerns in relation to the state of guardianship it may be necessary to contact the courts offices for verification. The legal basis for doing so must be very clear.

THere is also the issue of persons who may be working in the situation where they are acting in 'loco partentis' that is they are stepping into the shoes of a guardian. In many instances this may be done on foot of a court order, verification of this should be attained in order for proof.

Question 10

Prior to 25 May 2018, there was no law setting the age of digital consent in Ireland, but many online service providers required users to be at least 13. If an online service provider now is aware that an existing user of their service is under 16, should the user be locked out of the service until they reach 16?

The answer to this question depends on the nature of the service that is being availed of and the basis for processing, or whether an alternative basis for processing other than consent is available to be relied on.

Simply put, if the online service provider has another basis for processing under Article 6, then Article 8 does not apply and the "digital age of consent" need not be considered.

For processing activities which do rely on consent (e.g. marketing analytics, cookies etc.), the question is then one of what would be the most beneficial resolution for the data subject in this case. Certainly any "non-essential" components of the online service for which consent is the only basis for processing should be terminated (e.g. tracking or analytics cookies, profiling etc.). For other functions it may be possible to identify alternative grounds for processing and communicate those to the affected data subjects.

Given the potential impact on fundamental rights and freedoms (e.g. freedom of expression, freedom of association) of young people, providers who seek to identify such alternate grounds and offer a (perhaps curtailed) service to this category of data subjects should be able to cite this as a mitigating factor in any enforcement action that might be taken, and a non-fines based sanction under Article 58 of the Regulation would be appropriate in such cases.

However, it is an unescapable reality that any operator of an online service for which consent was the basis for processing who knowingly continues to process data of someone under the age of 16 is committing an offence under the Regulation and could face personal liability under Section 146 of the Data Protection Act 2018. A failure to act to remedy the situation would be a conscious decision or a negligent act on the part of the directors, managers, and officers of the body corporate in question. Pending any future change in legislation, this is the inescapable factual situation.

It would be significantly remiss of an independent regulator to issue guidance to organisations that there might be a blind-eye turned to infringements of this nature, however it would be a valid use of the discretion of the Office to take into consideration actions taken to adjust services to remove reliance on consent where possible.

Summary of Answer

Where consent is the only basis for processing the law is clear and it is not for the Regulator to seek to create a loophole.

However, it is in the capacity of Data Controllers to adjust their services and to take actions to remove their reliance on consent as the basis for processing in these contexts. Where this is possible, it should be done, and this may permit curtailed services to continue, but this would be determined on a case by case basis.

These actions should be considered as mitigating factors in the event of any breach of Article 8(1). Consideration should be given on a case by case basis to the balancing of the fundamental rights and freedoms of the child.

However, where no effort is made to remove or reduce reliance on consent as the basis for processing, the Office of the Commission has no alternative but to require processing to be ceased for this cohort of data subjects.

Question 11

How should such online service providers ensure they comply with different ages of digital consent in different Member States?

This is a question for the risk appetite of the online service provider and their available resources.

One option would be for the online service provider to pick the highest age and operate to that. This would be appropriate for resource-constrained operators or providers seeking to have a single standard operating process across their organisation.

Indeed, in the case of an online service provider operating under Binding Corporate Rules, it would be the case that the applicable age of digital consent that would apply to them would be the age of consent in the jurisdiction of their main establishment under BCR.

Another approach would be to use technological solutions such as rules-based triggering to apply the appropriate age based on the jurisdiction the data subject is identified as being based. This is not a fool proof solution however and could be 'gamed' by use of VPNs or falsified profile data. Therefore it may require secondary data checks to validate and verify the location of residence of the data subject. This would be similar to the operation of the VAT Directive and the requirement to verify the country of delivery of services to ensure the correct VAT rate is charged in online transactions.

Various solutions have emerged to the VAT challenge of different tax rates in online services and, should the rules-based approach be applied, it is inevitable that technical solutions will be come available to address this challenge in an innovative manner.

Summary of Answer

We deal with a similar challenge in the context of the VAT Directives. Technological solutions have emerged in that context and will emerge in this context.

Ultimately, the approach adopted will be constrained by the risk appetite and technical resources of the organisation, so development of a simple technical solution similar to Taxamo or the other online services for VAT management should be encouraged.

Question 12

In the case of marketing to a child, what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?

The marketing organization's legitimate interest is in marketing to the decision-making party with purchasing authority and power. In many cases, and particularly in any cases where the child is under an age equivalent to the digital age of consent, this person is the parent, not the child. In most cases processing the personal data of children for the purposes of targeting advertising is extremely inappropriate and contrary to the interests and rights of the child who is being marketed to.

Depending on the age of the child in question, a child may still be forming concepts of money and value and may have limited concept of the costs incurred. Additionally, direct advertising, in particular programmatic or targeted advertising (in contrast to broadcast advertising) may result in harmful stereotyping resulting in manipulation.

Processing children's data for marketing purposes or to target marketing to them runs the risk of "hidden" or covert communications to children that undermine parental ability to be aware of and understand the messages children are exposed to and provide guidance or assurance as necessary. The nature of current programmatic internet advertising technology increases the risk of filter bubbles, dark patterns, and manipulation. Any marketing should be done acknowledging that the balance of risk to the child vs. the legitimate interests of the organization is incredibly skewed against the rights and interests of the child, and that the duty of care on the part of the data controller is heightened due to risk.

Considerations should include:

- The necessity of direct marketing to a child
- Utility to the child vs. the invasiveness or intrusiveness of processing
- The level of cognitive development and social awareness of the child
- Capacity of the child to "consent"
- Capacity of the child to understand the ability to object
- Degree of manipulation
- Pressure on parents to provide
- Risk child incurring costs purchasing where payment card data is stored on devices
- Visibility of marketing to parents, in order to allow for open discussion and teaching regarding the functioning of marketing
- Degree of sophistication of understanding and media literacy of the child

- Degree of understanding of concepts such as delayed gratification and saving money
- Ability of the child to make their own purchases
- Degree of autonomy and social development of the child
- Type of product or service being offered / marketed

With checks and balances in place to protect the rights and freedoms of the child it might be reasonable to market directly to a child who is over the digital age of consent. In most cases, there would be no reason not to prohibit processing the data of children under the age of digital consent without the explicit consent of the parent.

Question 13

Should organisations be prohibited from profiling children for marketing purposes? If so, should this be age-dependent or dependent on other factors? If so, what are these other factors?

The key question here is who the marketing is really being targeted at, and the answer is that it is targeted at the person making the purchasing decisions or funding the purchasing action – the parent.

Historically (pre-internet) marketing to children was at a "macro" level based on the outlet or medium. Only in recent years have we had the ability to specifically profile and target children for advertising.

Given the potential for these profiles to persist and to follow children into their audlt lives, such processing should be considered excessive when the same result can be achieved by developing profiles of parents (with their consent).

As children are unlikely to fully appreciate the implications of this profiling and the potential impacts on the information they are presented with and have access to in online services, or even more worryingly are likely to interpret this abstract concept of "profiling" as a concrete action of being surveilled by unknown entities. Our managing director has experienced this with his own child and some of their friends when they developed an awareness of online tracking.

While the "Elf on the Shelf" seeks to normalise the mass surveillance of children in the interests of capitalism, there is no reason why legislation should permit this deep and pervasive invasion of childhood.

It is worth noting that the leading toy brand Lego does not engage in profiling of children using its online services as they consider this to be inconsistent with their core ethical values of creating safe spaces for children to play and develop their imaginations.

While age is the main factor that could be considered here, one might also consider level of cognitive development of the data subject and the potential for similar harm and invasiveness for people with learning difficulties or cognitive impairments.

Summary of Answer

There is no reason why the profiling of children should not be prohibited. The advent and evolution of the technology capability to do this is relatively recent, and leading child-focussed brands have opted not to implement it.

Question 14

What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children?

At all times where new products/services are being provided it is important to conduct thorough privacy impact assessments to include three main groups;

- People who have experience/expertise of working with children
- People who understand the intended product/service
- People with an expertise in data privacy

Input from these three sections will outline the vision of the product, the reality of children's needs, and the requirements of data privacy legislation. The idea is that at every step of evolution that the actions to be taken are informed from the view of both children and Data Privacy legislation and ethics.

Question 15

Do you think 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? For example, should there be stricter privacy settings for younger children? How should these variations in the privacy settings be given effect?

Defaults should always be to the maximum level of privacy. Communication should be clear and targeted to the age and understanding level of the child, to help inform them what the various privacy settings mean. It is also important to ensure that parents are empowered and informed about what settings mean, so that they can make decisions or guide the child as appropriate.

The expertise of child psychologists should be referred to here, regarding children's relational understanding of privacy and of social and technical interaction. Products default settings and degrees of processing of children's personal data should be designed with this in mind.

In the case of younger children, allowing the parent to set privacy controls that children may not override would be one stricter variation on privacy settings. It is reasonable to expect and allow older children and adolescents to exercise increasing levels of autonomy in social interaction, so stricter privacy settings for young children

with more reasonable options for older children and adolescents would be reasonable.

- What types of sharing or broadcasting of data might be allowed?
- What security and access controls are required?
- What access controls are required?
- Who is allowed to contact or communicate with the child? Who is the appropriate person to control and verify the contact/communication?
- What types of social groups or circles of contacts might be created for granular sharing of data to or within specific groups?
- Is parental approval required or appropriate?
- Is it desirable or reasonable to create a limit on access and communication only to people who have been physically verified as appropriate contacts?

Summary of answer

Defaults must always to be a maximum level of privacy

It is vital that both children and adults are informed and empowered to understand the privacy settings and how they can exercise control over their data.

Older children will require settings that allow them an increasing level of autonomy.

Question 16

Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation?

The modern family is one which may be subject to more fluid family dynamics than was traditionally the case. While there is an obligation on a controller to verify ID of guardian or relevant others it is the case that it may be next to impossible to do so in certain situations, therefore it may be that there is a risk to an organisation in a situation as they are unable to keep up with this and are found to be liable as a result.

Further it is likely that there is no solution that will be perfect and that the best option is to focus on the rights of the child and to provide guidance on individual situations, applying appropriate controls on a case by case basis.