QUESTIONS FOR PUBLIC CONSULTATION

The DPC seeks submissions in response to the questions set out in respect of each of the following issues:

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

(A) Transparency and the right to be informed about use of personal data (Articles 12-14 GDPR)

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.

ISPCC Opening Comment

The ISPCC is delighted to have the opportunity to feed into the Data Protection Commission's (DPC) 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).

The ISPCC engaged with its Children's Advisory Committees (CACs) to seek their thoughts on some of the questions outlined in this consultation, referenced throughout our submission. The ISPCC believes that children and young people should have the opportunity to be fully involved in setting priorities, developing strategies, assessing progress in their communities, preparing for adversities and taking part in decisions that affect their lives. These committees afford children this opportunity and we were delighted they were able to add their voices and opinions to our submission.

It is particularly welcome to see the principles of the United Nations Convention on the Rights of the Child (UNCRC) referenced by the DPC in the consultation. Moreover, it is very welcome to see that a second stream of the DPC's consultation will be with children.

The ISPCC is available to furnish the DPC with any additional information based on its submission.

Questions:

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

1.1 The principle of transparency as it pertains to the GDPR and children outlines the importance and necessity of presenting information relating to the processing of their personal data in an accessible manner, using child-friendly language that is easy to understand.

1.2 Organisations processing children's personal data could support educators in designing effective education programmes. In order to develop education modules that cover data protection, educators need to have a much more in-depth knowledge of how and for what reasons organisations process children's data to design the best programmes to support children's data protection learning.

"This information should just pop up on the screen, for example, when downloading a new app on your personal phone; a pop up of information should come up on the screen and you have the option to agree or disagree. It should not for example, on [social media platform] it brings you to your [email provider] account and then back to [social media platform] - this is not convenient.

The notice needs to be short and brief, otherwise people will not read the information and sign up to something that they are unaware of. For example, [brand of phone] have up to 6-8 pages of terms and conditions and this information is not child friendly or easy to understand. At the end of the day we really do not know what our personal data is being used for", ISPCC CAC

1.3 Organisations should put in place mechanisms to consult with children on the development of their privacy notices along with any other information and communications on the processing of children's personal data, and to test the robustness of same. Organisations should be encouraged and supported to consult with children when reviewing and updating their transparency notices, too.

1.4 It is imperative children are aware what behaviours and habits of theirs are being tracked and how this information is being used (i.e. is it being shared with a third party and if so, for what reason).

1.5 Child-friendly and easily digestible transparency/privacy notices/communications could include infographics, symbols and short videos/cartoons using clear and plain language conveying how and for what reasons the child's personal data is being processed. Videos showing the pathway of data processing could also prove useful, including visual aids on how to withdraw consent, where consent is the legal basis for processing.

1.6 Organisations should also show how their product or service can be used without a child having their data being processed, if applicable.

1.7 Organisations should provide a dedicated contact email address should children be concerned about how their personal data is being processed or have any other queries regarding same.

1.8 Any transparency notice should show how the organisation plans to respect all children's individual data protection rights.

"Bullet points, not long paragraphs that are difficult to read & understand. 'We will be collecting and storing your data, this is what it can be used for…' To the point, just tell you outright and not have it hidden at the very bottom of a page", ISPCC CAC

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

2.1 It is incumbent on organisations to establish the makeup of the audience at which its service or product is aimed, and take the right steps in providing transparency messages for both. 'It should also involve an evaluation of the appropriateness of electronic tools such as layered information notices, pop-up notices, hover-over notices or voice alerts'.

2.2 If their products and services are aimed at both audiences, then two separate sets of transparency information notices/communications could be provided to meet the needs of each audience. The information should be the same for both, but in a more child-friendly manner for children and vulnerable adults. Useful approaches as outlined in point

1.5 could also be used here, i.e. infographics, symbols and short videos/cartoons using clear and plain language.

(B) Right of access (Article 15 GDPR)

The right of access is one of the most important data protection rights because it allows individuals to find out whether their personal data is being held by a specific organisation and to obtain a copy of their personal data.

Like all other data protection rights, the GDPR does not say when, or in what circumstances, a parent or guardian can make an access request for their child's personal data, or when or in what circumstances a child can make their own access request for their personal data.

Questions

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?

A child should be able to make an access request to an organisation once they have reached a level of maturity and understanding of their rights and responsibilities. 'In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown.'[1] If an organisation is satisfied that a child has attained a level of maturity and understanding about their rights, they should then endeavour to vindicate those rights.

Some suggestions for consideration covered in the ICO Guidance in the UK include[2];

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to exercise the child's rights. This is particularly important if there have been allegations of abuse or ill treatment;

[1] 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/
[2] Ibid. Pg. 41

- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

"Maturity should be taken into consideration for example an 8 year old would not understand this topic, however, a 13-14 year old has a better level of maturity and understanding. That is a genuine request coming from the individual and not a person illegally trying to access someone's personal information. How the organisation would determine this- we do not know. For example, a young person who is being bullied and the bully is trying to frame the victim or hack their personal site [social media platform], the organisation would need to have security measures in place to determine it is genuine", ISPCC CAC

"Their age, but not sure if there should be any real restrictions, there would be a reason they want the data, we don't feel very young kids would be looking for it, if it's your information, you should have the right to have it", ISPCC CAC

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?

4.1 The right belongs to the child and their best interests should always be taken into account, but some children may not be able to exercise their rights for various reasons.

4.2 A parent should be able to make an access request and to receive a copy of their child's personal data at the request of the child, and/or with the child's awareness and consent, where possible.

4.3 There may be circumstances where the child is unable to acquiesce to have the holder of parental responsibility support an access request situation: perhaps if the child is particularly vulnerable; lacks competence; lacks maturity or understanding of the significance of sharing their personal data and having it processed, or are unable to understand the risks or consequences of having their personal data processed.

"If a parent had a genuine concern that their child was being bullied online and the bully was using their personal data. Or if the young person's personal data was being hacked, in these cases the child must give written consent to allow the parent to access their personal data. If a child was in foster care, this situation would depend if the child has regular access with their parent and a good relationship. Also written consent needed from the child", ISPCC CAC

"If they are concerned about something. Maybe they should have the permission of their child about accessing the personal data, depending on the child's age. If their child is at immediate risk and they need the personal data", ISPCC CAC

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?

5.1 The right belongs to the child and their best interests should always be taken into account, but some children may not be able to exercise their rights for various reasons.

5.2 Please see list referred to in Q.3.

5.3 The UN Committee on the Rights of the Child issued a guidance on determining the best interests of the child.[3] This guidance could act as a basis for organisations developing a uniform mechanism for achieving balance.
Regarding safety it states:
'73. Assessment of the child's best interests must also include consideration of the child's safety, that is, the right of the child to protection against all forms of physical or mental violence, injury or abuse (Art. 19), sexual harassment, peer pressure, bullying, degrading treatment, etc., as well as protection against sexual, economic and other exploitation, drugs, labour, armed conflict, etc.(arts. 32-39)'.

[3] https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf

(C) Right to erasure ("Right to be forgotten") – Article 17 GDPR)

Individuals have the right to have their personal data erased, without undue delay, by an organisation if certain grounds apply. This includes where personal data was collected by an online service provider in circumstances where the individual now making the erasure request originally gave their consent to have their personal data used or collected when they were a child. The GDPR says that where this has happened, an individual should be able to request that their personal data be erased because, having been a child when they consented to the collection and use of their personal data, they may not have fully understood the risks of doing so.

Questions

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?

6.1 The concept of 'sharenting' is a relatively new phenomenon: parents sharing their children's data (images and other personal information about their children) publically online, usually without their child's consent. Commonly shared images include children's birthday parties (gives age of child); first day of school (logo on uniform can identify a child's school); holiday photos (can show a child's location) and so forth. Even if the – innocently shared – information is not as obvious as these examples, there is often quite a lot of metadata attached to these images: behind the scenes data that is easily accessible and can illicit the same potentially identifying information, and more.

6.2 In a recent media report, self-generated imagery (sex videos) created by children is reportedly being shared by paedophiles online without the knowledge of the young people who created it.[4]

6.3 These are just some examples of where the ISPCC believes children should be able to exercise their 'right to erasure', notwithstanding cooperation from parents to remove 'sharenting' images at source.

6.4 This can be at an age where they express their upset or concern at the data shared; there is an awareness of their rights or their rights have been explained to them; exercising the right is offered as a potential remedy to the situation, and they wish to exercise it.

[4] Aaron Rogan (2019) 'Teenagers sex videos shared by paedophiles' *The Times (Ireland Edition)* 16 February, Front Page

6.5 Social media companies should have polices in place to deal with requests to remove content, but these are not always effective and efficient. If the request to remove/takedown content does not meet their terms and conditions it can be difficult or in some cases impossible to get the content removed, and therefore for the child to have their 'right to erasure' vindicated. A social media provider's obligations are to remove illegal content as per the eCommerce Directive, and not other types of content or 'sharenting' content children may want removed.[5] Sometimes images are shared which could potentially cause embarrassment to the child. 'By age four, children have an awareness of their sense of self'.[6]

6.6 Nevertheless, the data belongs to the child and not the parent, even though it is generally accepted that parents are considered the 'gatekeepers' of their children's personal information.[7]

6.7 The guidance from the DPC regarding a child's right to erasure should require social media companies to recognise this right in the light of this content, and remove the type of content outlined above should the data belong to the child and was shared without their consent; if the data was shared with their consent, then the company has to recognise the child's right to withdraw their consent and remove the content anyway. The ISPCC recognises there are limitations to the 'right to erasure'.

6.8 DPC guidance for parents should address the issue of 'sharenting': what it is and why parents should think before they post; the importance of consulting with their child, where appropriate and the potential risks with sharing information that does not belong to them and how to recognise and respect their child's right to privacy.

6.9 'Right to erasure' should be considered for children no matter what the content is: if it is their personal data, they own it and therefore have the right to have it erased, taking into account certain exemption circumstances as outlined in the text of the GDPR.

"If someone made a fake page on the child; If they are no longer engaging with the app or the organisation; To send an email to the child asking them this question and allowing 30 days to respond; If the child no longer consents to receive a service from the organisation", ISPCC CAC

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[6] Communications Law - Journal of Computer, Media and Telecommunications Law Vol. 23 No. 1 2018 Pg. 7.

[7] Ibid. Pg. 18

"Not sure, but maybe if a child wants their data deleted then it's their choice and once they are sure they understand that it will be gone then it's up to them, again depending on their age", ISPCC CAC

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?

Parents can be the most usual and effective advocates for their children, in terms of making decisions for the safety and wellbeing of their children, particualrly in circumstances where the child is not mature enough (not necessarily based on age attainment). A joint request may be preferable at an upper age level. Parents acting in the best interests of their child is paramount.

The circumstances outlined below are similar to those mentioned earlier for a parent making an access request on behalf of their child.

7.1 The right belongs to the child and their best interests should always be taken into account, but some children may not be able to exercise their rights for various reasons.

7.2 A parent should be able to make an erasure request on behalf of their child at the request of the child, and/or with the child's awareness and consent, where possible.

7.3 There may be circumstances where the child is unable to acquiesce to having the holder of parental responsibility support an erasure request situation. Perhaps if the child is particularly vulnerable; lacks competence; lacks maturity or understanding of the significance of sharing their personal data and having it processed, or are unable to understand the risks or consequences of having their personal data processed.

7.4 If a child had previously consented to their personal data being processed but now wanted to withdraw that consent but was unable to, parental support may be useful and could result in the parent having to make an erasure request.

"If there were specific reasons and the child's safety was in question. For example if the child was being bullied online and they had proof of this through screenshots", ISPCC CAC

"If there is a risk or concern about the child. If the child wants the data removed", ISPCC CAC

II. Safeguards (A) Age verification (Article 8 GDPR)

In Ireland, children below the age of 16 (the "age of digital consent") cannot give consent to online service providers to process their personal data. If consent to process personal data is requested by the online service provider in order for the child to access the service, parental consent must be given. This means that 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".

Questions

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?

8.1 There are few, if any examples of age-verification methods for children (under 18s) that can reliably verify a child is over 16 years, Ireland's 'age of digital consent'. There is much evidence to show that children tend to lie about their age in order to access online services, services offered directly to them or easily accessible by them, which has further implications for their overall protection, including their data protection.

8.2 Verification methods could possibly include the use of some form of official ID (although these are limited in the case of minors) – a passport, a student card, a Garda ID card. 'Any data collected by organisations to this effect, and which is not required for evidential purposes and has no other function, should be immediately deleted following verification, to ensure compliance with the principle of data minimisation.'[8]

8.3 Secure third party verification methods could be employed should they respect data protection principles.

[8] GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership 6 March 2018, Pg. 15

"*To show proof of ID for example, student card which can be given from 12 years up. To send a screenshot of this ID to verify the child's age. To connect the child's [social media platform] page to their parents page to verify their age*", ISPCC CAC

"Contact parents/guardians. Could ask for year of birth maybe but that can be difficult to prove or someone can make one up to appear older", ISPCC CAC

9. (a) 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?

9.1 'The FTC [Federal Trade Commission, US] has approved the use of several methods to ensure that the person giving the consent is the child's parent.[9] These include:

- sign a consent form and send it back to you via fax, mail, or electronic scan;
- use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
- call a toll-free number staffed by trained personnel;
- connect to trained personnel via a video conference;
- provide a copy of a form of government issued ID that you check against a database, as long as you delete the identification from your records when you finish the verification process;
- answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or
- verify a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology..'

9.2 Organisations should assess the risk level posed by their data processing methods/rationale and should assign a method of parental consent accordingly.

9.3 Organisations need to respect the principle of data minimisation and should delete parental consent information once its purpose for acquiring it has been fulfilled.[10]

[9] US Federal Trade Commission, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business", https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

[10] GDPR Implementation In Respect of Children's Data and Consent Centre for Information Policy Leadership 6 March 2018, Pg. 15

"*Emailing a parent for permission and the parent has to read through the information and give it the ok at the end. Could also be done through a phone call.*
One member had experience of signing up for some software and this is how it was handled when she put her age in they asked for a parent's email and her mom had to agree to give permission. It worked well.
Even though there's a chance people might not give their parent's [email] address, the organisation has clearly asked for that to be done", ISPCC CAC

"*Internet sites are getting better at this but there will always be ways around accessing sites under 16. If [social media platform] connect the child's page to the parents [social media platform] page and send an email to the parent to verify this*", ISPCC CAC

(b) 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?

A 'reasonable effort' made by organisations should be determined on the risk attached to the type of processing on the child's personal data. If the risk is high then the efforts by the organisation to verify the holder of parental responsibility should reflect this approach.

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 'age of digital consent' in Ireland is 16 years meaning it is unlawful for organisations to process personal data of children without the consent of the holder of parental responsibility, where consent is the legal basis.

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

Many online service providers offer services in multiple EU countries where there are different ages of digital consent. For example, while the age of digital consent in Ireland is 16, in Spain it is 13, and in Austria it is 14.

Questions

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

Where organisations are highly adept at tailoring content to age, demographic, profiling, etc. similar technology could be employed to ensure compliance with different ages of digital consent in different Member States.

Where a service is usually offered to all Member States then perhaps a mechanism could be put in place to determine what 'age of digital consent' jurisdiction the child is in.

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

Profiling is 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. For example, organisations may collect information from their customers or users to try to predict other services or products they might be interested in.

A user profile can be a really 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 information, advertisements and marketing materials, amongst other things, precisely to a person's interests, needs or individual views. For example, if an individual often clicks on posts online about a specific singer or "likes" pictures of clothes from a particular shop, they may start to see ads for tickets to that singer's concert or similar artists' concerts popping up on their social media feed, or ads might start appearing telling them that there is a sale on in that particular shop or similar shops. That is because online operators are constantly collecting and frequently sharing with each other this type of information about users and adding it to the profile being built about them. In this way, the user's profile then becomes the basis upon which specific advertising and marketing materials are selected to target that user.

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.

Questions

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 GDPR is clear that children's personal data merits specific protection. If an organisation feels it is within their legitimate interest to directly market to a child and have carried out the appropriate risk assessment of doing same to ascertain the risk to the rights and freedoms of children, then they should consider the following factors:

12.1 The processing should be fair and recognise that children's personal data merits specific protection.

12.2 There should be a level of transparency attached to any direct marketing based on children's personal data: the organisation should be explicit in *how* the content of the direct marketing is determined.

12.3 A young or vulnerable child's lack of understanding should not be exploited for commercial gain. Children are impressionable and may not have the critical analysis skills to understand what is behind this type of marketing, and perhaps make choices they would not have if their personal data was processed in a particular way. The Advertising Standards Authority of Ireland in its Code has useful guidance on advertising and marketing to children, which could be considered when creating this guidance.[11]

12.4 Children should be reminded they have the right to object to their personal data being processed for direct marketing purposes, with clear opt-out options available without incurring punitive measures to the provision of the service or the functionality of the product.

12.5 Rewards or incentives should not be used as a ploy to encourage children to not object to the processing of their personal data.

[11] https://www.asai.ie/asaicode/section-7-children/

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?

13.1 The Article 29 Data Protection Working Party states that children are a vulnerable group and 'organisations should, in general refrain from profiling them for marketing purposes.'[12]

13.2 The ISPCC agrees with this position and believes that organisations should be prohibited from profiling children for marketing purposes. Some older children may be aware of how their personal data is processed (profiled) in order to market to them and to advertise to them, but children in general lack this knowledge, i.e. if data is being processed to drive behavioural advertising a child may not understand this. There is little on the school curriculum that covers this area of online safety.

13.3 Some of the young people we consulted with felt strongly that organisations should be prohibited from profiling them:

"Yes, it is personal data. These things need permission and it is creepy that they can profile you from your personal data", ISPCC CAC

While others, felt differently:

"Could it be a choice for the young person if over 16 and if under 16 could it be asked of the parent when they are emailed", ISPCC CAC

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.

[12] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 Pg. 29

Questions

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?

14.1 Article 3 of the United Nations Convention on the Rights of the Child (UNCRC) recognises that 'In all actions concerning children…the best interests of the child shall be a primary consideration."[13]

14.2 While the Council of Europe's *Guidelines to respect, protect and fulfil the rights of the child in the digital environment* recognise that 'States should promote and provide incentives to business enterprises to implement safety by design, privacy by design and privacy by default as guiding principles for products and services' features and functionalities addressed to or used by children.[14]

14.3 The GDPR clearly states in Recital 38 that children merit specific protection by the very nature of them being a child.[15]

14.4 Ireland's Data Protection Act 2018 specifically states that any reference to a 'child' within the Regulation be taken as reference to a person under 18 years of age.[16]

14.5 Organisations employing robust data protection by design and by default should consider the following when developing services/products aimed at children:

- Highest privacy settings as standard across all services/products aimed at children; opt-in options for lowering these settings, with a clear statement of what this means (transparency principle).
- Only minimal personal data processing should be required to register for a service/product (data minimisation principle).
- Data pseudonymisation should be used where data processing is required on multiple types of personal data, including sensitive personal data (data pseudonymisation principle).

[13] https://www.ohchr.org/en/professionalinterest/pages/crc.aspx
[14] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a Pg. 20
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[16] http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/pdf Section 29

- Organisations should use Data Impact Assessments (DPIAs) to consider if their processing will infringe on the rights and freedoms of children, given the special consideration children's data is given by Recital 38.
- Consideration should be given to publish the outcomes of these assessments, for reasons suggested by the Article 29 Data Protection Working Party [17] and the Irish Data Protection Commissioner.[18]

14.6 All organisations processing children's personal data (i.e. any person under 18 years of age) should use DPIAs to assess potential risks associated with the processing of children's data and to plan robust mitigation strategies against these risks, given the special consideration children's data is given by Recital 38.

"*Keeping personal data to a minimum for example, only using name and age. Not to use address or phone number that is creepy*", ISPCC CAC

"Have it in place from the very beginning and clearly outline data protection, don't hide it, use child friendly language, being honest about it", ISPCC CAC

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?

Yes, products and services that are used by or offered to children should have built-in default privacy settings regardless of the age of the child.

It may be difficult to give effect to variations in privacy settings with technology, given that children grow and develop at different rates, recognised in the UNCRC and the evolving capacities of a child. Consideration could be given to holders of parental responsibility to manually opt-in to lower privacy settings as younger children's capacities evolve; older children who have the capacity and competence could opt-in to lower privacy settings for products and services themselves.

[17] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 Pg. 18
[18] http://gdprandyou.ie/data-protection-impact-assessments-dpia/#should-the-dpia-be-published

V. General

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

16.1 The ISPCC believes that this guidance should be child-centred and developed with a child's rights perspective, based on the rights and principles of the UNCRC. Children are important stakeholders in how organisations process their personal data and have the right to have their opinions heard and taken into account.

16.2 As the GDPR is a principles based law and is open to interpretation for the most part, the DPC could develop a set of standards which model best practice for organisations that need to provide 'appropriate measures' and make 'reasonable efforts' to uphold children's data protection rights.

"*There is a conspiracy theory from [name supplied] on the online world and this has created fear and worry in some children. More children and young people are aware of webcams on laptops, tablets and phones and the dangers around them*", ISPCC CAC

"*To be clear on what data is collected, child friendly explanation", Cork CAC Member*

Final Comment

The ISPCC has been to the fore in calling for online safety education to be embedded in the school curriculum, from primary level. Any online safety education programme should include children's data protection rights: what is personal information; reasons it can be processed; how to recognise when their personal data is processed (e.g. targeted marketing,); leaving a digital footprint, along with the potential risks of their personal data ending up in the wrong hands.

In order for children to truly have agency over their data protection rights;

- Organisations need to offer better transparency on how they process children's personal data.
- Educators need to be better informed in designing relevant programmes.
- Holders of parental responsibility need to have a greater awareness of their children's personal data and how it is processed so they can offer the necessary guidance to support children in this area.