Public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation

CybersafeIreland response to the questions provided on the DPC Consultation Documents

Questions:

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

Data collection and use is usually communicated in lengthy hard to understand terms and conditions and privacy policies. An awareness video could be an effective way to communicate this information to children. It is important for children to start understanding the reality of what is going on behind the scenes when they are online at an early age. If they cannot understand this in reality they should not be taking part in activities online that require their personal data to be collected. The idea of an awareness video is that it would enable the children to be able to visualise "personal data". They will not have the education and knowledge to be able to read and understand lengthy policies so this information must be delivered in a way that is comprehensible to their age group. A quiz could be present at the end of the video to ensure they understand what personal data is and explain this is what they are giving away by using this service.

Ideas – digital footprint cartoon video of a polar bear leaving footprints of data for everyone to see. Must include consent explanation and overview of consequences.

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?**

Most internet users do not read the terms and conditions and privacy policies that provide information before agreeing to them. Because of this it can be assumed that a large proportion of internet users have limited idea of what is happening to their personal data (and activity/browsing data)

An awareness video may be the best option for adults also. For example, is the site selling it onto brokers, do third parties have access?

If not a video, then a narrative piece written in very concise, clear and easy-to- understand language would be needed.

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?**

This could potentially happen at any age as long as it is with parental consent but in order to do it independently it would make sense to put it in line with the digital age of consent although in our view this should be set at 13 rather than 16 in Ireland.

Developmental stages should play key factor here.

Industry vs. Inferiority

During the elementary school stage (ages 6–12), children face the task of *industry vs. inferiority.* Children begin to compare themselves with their peers to see how they measure up. They either develop a sense of pride and accomplishment in their schoolwork, sports, social activities, and family life, or they feel inferior and inadequate because they feel that they don't measure up. If children do not learn to get along with others or have negative experiences at home or with peers, an inferiority complex might develop.

This also relates to data shared by others about the child online. For example a parent or caregiver may have shared much of a child's upbringing online. At this important development stage where a child is beginning to compare themselves and develop a sense of pride because of their lives or develop a sense of inferiority. These photos may have detrimental effects on this child's psychological wellbeing. It could lead to isolation and cyberbullying. "Selfie culture" what if your parents have shared not so perfect photos since the child born? The parent has therefore potentially shared an identity for the child, not allowing them to develop their own identity and sense of self which is important at this young impressionable age.

CybersafeIreland has found plenty of anecdotal evidence through its work in schools that girls as young as 9 rely heavily on the online validation, for example, deleting photos that don't get enough likes on their social media pages or if there is mean comments on the photo.

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?**

Parents should be able to make an access request under exceptional circumstances at any age although it would make sense for children to be able to make their own request at the age of digital consent (with a better evidence base of what that should be). Algorithms are making fundamental choices based on the data feeding them which means it is essential for the data to be accessible to parents.

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?**

This is difficult as it depends on the context, from one extreme to the other. It should also depend on the age of the child.

Does a gaming application really need personal data to play to game in the first place? If the gaming application has collected data on a child, the parent should be able to access this up until 16 (or 18) if they think it is necessary for the protection of the best interests of their child. Additionally, games have recommended ages (PEGI) so this could be taken into consideration of who has rights to what. Nevertheless, if the game can be played without personal data there is no reason for the game to collect it in the first place.

Social media, this is where the child's right to privacy has to begin. Social media is now the main source of communication for children, they often socialise and 'hang out' on these platforms. Part of growing up and developing into an adult is being independent, and it is important that children in this day and age are allowed to do this. At a certain point, it would not be fair for their parents to have total control over this though we would encourage building a relationship of openness and

ultimately trust between parent and child. We encourage parents to prepare their children for greater independence in the online world at the right point (and that can vary depending on the child). Social media platforms decide an age that it is safe for children to use their platforms, although this can often feel quite randomly selected and there is little evidence to suggest that there is an "ideal age" for access to these service or more independence on them. It will often depend on the child.

There also needs to be circumstances if parents are worried over the welfare and mental health of their child, the social media platform should be able to inform the parent if the child is under 18.

How much privacy does a child have right to? Age and context dependent.

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?**

Any age and this can be with or without parental consent after a certain point (digital age of consent?). One form of cyberbullying is the bully posting a not so flattering photo of the victim on social media, it is important that the person in the photo is allowed to request this damaging photo to be erased. The consequences from acts like this have been devastating and it has been reported in media that they have led to self-harm and suicide. It is well known for years that bullying has negative consequences for the victim. Sharing of others data such as photos, videos and other material needs to be discussed with children – it can have severe negative consequences. Including, reputational and psychological damage.

Don't judge a book by the cover has now turned into judging people by their social media accounts, it is important children control their own identities allowing them to develop a sense of self and independence and not allowing others (bullies) decide this for them.

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?**

Up to the digital age of consent (which should be 13), it should be up to the parent.

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?**

We believe that we need to get to a place where children can be honest about their age when they sign up and if they are under 16, then all sorts of protections should follow (educational pop-up messages, absolutely zero collection of data, appropriate filtering etc).

(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?

Proper identification, unfortunately it seems to only way to properly identify another person but see point above about children being allowed to be honest about their age.

(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?

The current situation clearly underplays it – they are choosing to exercise a light touch in most cases.

Much better educational offerings on their websites platforms for underage users.

There are also technical means of determining if a user is under a certain age just by how they use the services, what they post etc.

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?**

They simply shouldn't be allowed to collect any data and there should be a safer user experience for those under the minimum age. Children under 16 can use these services, as long as they have (in theory) parental consent. It is our experience that many children do get this consent from parents but that it is not necessarily informed consent on the part of the parent.

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

This should be covered at the consent process of the terms of the site, the same way they verify age then. The social media platform should have edited versions of the agreement process when signing up depending on the country.

Clear T&Cs

More educational offerings for those under 16

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?**

Again, if children could be honest about their age it should trigger only age-appropriate or better still, no marketing as so many children we talk to are affected negatively by the advertising (on the basis that it's scary sometimes – drink driving ads or horror film ads, or that it's encouraging them to want things that aren't appropriate).

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 issue is the inappropriate content online that is making its way to children. Ideally it should be age-appropriate or not at all.

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**?

Privacy by default on apps and games

Geo-location services off by default

Honesty about actual age to trigger age-appropriate educational messaging and filtering, no ads etc

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?

This would be challenging. Privacy settings should simply be on for all users and it's then up to them to change that within the settings other than the current situation of everything being off. Evolving capacity of child should mean that they get more adept at deciding how much privacy they want!

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

Education and explanation needs to start of young, this is the world these children are coming into and have the right to be taught how to navigate their way safely around it. Cars were not banned after it was discovered they could crash; seat belts were installed then air bags as well as really informative education campaigns aimed at changing the way we use them.