

Response to the Consultation Paper “Data protection safeguards for children (‘digital age of consent’) from the Department of Justice and Equality.

Response

It is widely accepted that it is both important and complex to consider the impact of technology on human behaviour. This is largely the concern within the field of cyberpsychology, a now established field of study at the interface of psychology and technology. It is a field that is ideally positioned to offer rigorous insights into the issues directly of relevance to the consultation on the digital age of consent for Ireland.

We welcome the consultation that has been undertaken by the Department of Justice and Equality in relation to the digital age of consent. The new European General Data Protection Regulation (GDPR)¹ comes into effect in May 2018. The issue of the age at which children have rights to online media, and at which they can consent to profiling and data processing is of critical importance, in particular, for the well-being of children. Clause 1 of Article 8 (Conditions applicable to child's consent in relation to information society services) of the GDPR reads as follows:

“Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.”

Recital 38 of the GDPR notes:

“Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.”

We note that Ireland lacks coherent policy and educational protocols in relation to stages of ‘cyber cognitive development.’ Setting an appropriate digital age of consent is a complex

¹ http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2016_119_R_0001&from=EN

issue and it is important that we consider the matter carefully. In setting an appropriate digital age of consent, policy must be informed by role and the impact of technology has on cyber cognitive development so that we avoid placing children in positions in which they neither have the digital skills, nor the understanding of the consequences, of exercising digital rights without the required advice of a parent/guardian. This is particularly true in the context of social media. We are aware that the lower bound on the digital age of consent mentioned in the GDPR has its roots in the Children's Online Privacy Protection Act (COPPA)² in the United States, which places restrictions on the collection of personal data from children under the age of 13 without the verifiable consent of a parent or guardian. We also note that to date the COPPA regulation has not been rigorously adhered to, or enforced.

There are many different and inconsistent age-based definitions of a child. For example, US immigration defines a child as an individual under the age of 21.³ The UK, for child protection purposes, defines a child as an individual less than 18 years.⁴ In Ireland, 2001 Children Act⁵ also defines a child to mean a person under the age of 18 years. German youth protection initiatives apply to children under the age of 14 (Internet Content Governance Report⁶):

"A regulatory response to age-inappropriate content is provided by the example of Germany's youth protection system for the media, comprising a strict set of rules governing audiovisual, broadcast, gaming and online content. As a federal republic, Germany's Kommission für Jugendmedienschutz (KJM) (Commission for Youth Media Protection) acts as a central authority for Germany's sixteen Länder to set standards for the rating of content and monitoring of compliance under Germany's Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting"

The UN defines child as *"a child means every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier."*⁷ In general, settings in which child protection issues are of relevance, the age-based definition of a child is higher, which is appropriate. The concerns related to children in the context of the GDPR should be seen through the lens of child protection given the risks they are exposed to, and the impact they might have. The requirement for verifiable parental/guardian consent for those under the digital age of consent seems entirely appropriate and responsible, although it is fully acknowledged that an organisation can only go so far in assuring itself that such consent has been given. However, we believe parents/guardians are best placed to properly evaluate when it is appropriate to grant consent on behalf of their child. It is only they who can appropriately assess an individual child's level of maturity, understanding, and judgement in an online context.

² https://www.ftc.gov/sites/default/files/documents/federal_register_notices/16-c.f.r.part-312-childrens-online-privacy-protection-rule-proposed-rule-request-comment-proposal-amend-rule/110915coppa.pdf

³ <http://www.hooyou.com/definitionofchild/index.html>

⁴ <https://www.gov.uk/government/publications/safeguarding-children-and-young-people/safeguarding-children-and-young-people>

⁵ <http://www.irishstatutebook.ie/eli/2001/act/24/section/3/enacted/en/html#parti-sec3>

⁶ <http://www.dccae.gov.ie/communications/en-ie/Pages/Publication/Internet-Content-Governance-Advisory-Group-Report.aspx>

⁷ http://www.unicef.org.uk/Documents/Publication-pdfs/UNCRC_PRESS200910web.pdf

Why is 16 the maximum? If you search for the EU justification of age 16, little information is available. However the ICT Coalition⁸, which is made up of 20 companies from across the information and communications technology (ICT) sector including Facebook, Google, BBC, Vodafone. etc., issued a statement⁹ saying:

"Negotiators raised the age without engaging in stakeholder consultation, nor providing a rationale for raising the age to 16. Negotiators have rushed this amendment without soliciting any meaningful input from stakeholders, including child safety organizations. Stakeholders should have the opportunity to weigh in on this important change. In some member states, this closed door process may permit challenges via judicial review. Negotiators should also explain the rationale for raising the age to 16; to date no explanation has been articulated."

But, of course, the justification for 13 has never been presented either, apart from it being the age specified in COPPA in the USA, notably when the matter was debated and discussed not all parties actually agreed that 13 was the optimum age¹⁰.

An optimum digital age of consent for Ireland can be informed by best practice in other countries (e.g Jugendmedienschutz in Germany) and by the significant international body of literature regarding the age of consent for sexual activity, notably at 17 Ireland has one of the highest ages of consent in the EU. Additionally the Irish digital age of consent must be informed by the Law Reform Commission's 2011 Report on Children and the Law: Medical Treatment (LRC 103-2011)¹¹. The report recommended that 16 and 17 year olds should be presumed to have the capacity to consent to medical treatment. Regarding persons under 16, it was concluded that there should **not be** a presumption of capacity to consent, but that such capacity could be established in an individual case by reference to the person's maturity and his or her appreciation of the nature and consequences of the health care decision in question. The 2011 report therefore involved the application of a "mature minor" test, which has been applied, in a number of states, sometimes in case law and sometimes in legislation, to a wide variety of legal areas involving decision-making capacity of children and young persons. The "mature minor" test is sometimes equated with the phrase "Gillick competence" after the UK Gillick case (1985), where it was applied in the limited context of access to contraception, but it has a much wider application.

It is also worth noting that Article 42A of the Constitution (inserted by the children's rights referendum) also recognises the concept of a "mature minor" test, but again in a limited context. Article 42A provides that, in any of the court proceedings to which it applies (which are: (a) brought by the State, as guardian of the common good, for the purpose of preventing the safety and welfare of any child from being prejudicially affected, or (b) concerning the adoption, guardianship or custody of, or access to, any child), the following "mature minor" test is to apply:

⁸ <http://www.ictcoalition.eu/members>

⁹ <http://www.ictcoalition.eu/gallery/96/Briefing-Note-Age-of-Consent-in-the-General-Data-Protection-Regulation%5B3%5D.pdf>

¹⁰ https://www.ftc.gov/sites/default/files/documents/federal_register_notices/16-c.f.r.part-312-childrens-online-privacy-protection-rule-proposed-rule-request-comment-proposal-amend-rule/110915coppa.pdf

¹¹ <http://www.lawreform.ie/fileupload/Reports/Children%20and%20the%20Law103%202011.pdf>

“in respect of any child who is capable of forming his or her own views, the views of the child shall be ascertained and given due weight having regard to the age and maturity of the child.”

Whilst Article 42A may not directly apply to the age of consent for the purposes of the GDPR, the fact that the Constitution now includes a “mature minor” test is worth noting, and indeed may provide a basis for legal challenge regarding an inappropriate Irish digital age of consent.

Furthermore in a psychological context developmental stages are not achieved on specific dates (for example by the age 13), rather age bands or ranges are employed to allow for individual maturation process. That said, legal instruments need to focus on a specific age, for example the definition of a minor (person under the age of 18). If a developmental milestone must be enshrined as a legal and definitive age specific construct, then it would be advisable to adopt a protective stance, and legislate towards the upper end of the relevant age band, thereby affording protection to those who may be less mature or vulnerable.

The choice of where to set the digital age of consent needs to be informed by a very solid and mindful policy and educational perspective that is culturally specific. This requires measures focused on supporting and assessing stages of cyber cognitive development in Irish youth. We believe that Ireland needs to put in place a policy framework and an associated educational programme that ensures that our children are sufficiently aware and responsible to understand and exercise their digital rights by the time they reach the digital age of consent. In the absence of a rigorous basis for any specific age at this point, a prudent approach is to support the position that the digital age of consent in Ireland be set at 16, the default (and maximum) permitted under the GDPR.

[REDACTED]

[REDACTED]