Technology Ireland
Ibec

Making Ireland a global technology powerhouse

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: +353 1 605 1500
fax: +353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

5th April 2019

RE: PUBLIC CONSULTATION ON THE PROCESSING OF CHILDREN'S PERSONAL DATA AND THE RIGHTS OF CHILDREN AS DATA SUBJECTS UNDER THE GDPR

To whom it may concern,

Technology Ireland welcomes the opportunity to respond this important public consultation on issues relating to the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation (GDPR).

Technology Ireland is an Association within Ibec, which represents the ICT, digital and software technology sector. The Association is a pro-active membership organisation with over 200-member companies located throughout Ireland. We advocate on behalf of Ireland's indigenous and foreign direct investment technology companies to Government and policy makers.

Technology Ireland acknowledges that data protection law is about everyone's fundamental right to the protection of their personal data. When personal data is shared with an organisation, the organisation has a duty to comply with certain laws and obligations governing how that data is handled. We acknowledge too, that children enjoy all the same rights as adults over their personal data – data about them is still their personal data and does not belong to anyone else, such as a parent or guardian.

We hope our responses provide a balanced, considered and proportionate response to the child-specific protections attached to the provisions under the GDPR.

Kind Regards,

[redacted]

[redacted]
Acting Director
Technology Ireland

Technology Ireland
Ibec

Making Ireland a global technology powerhouse

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: + 353 1 605 1500
fax: + 353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

RESPONSE TO PUBLIC CONSULTATION QUESTIONS;

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

Different methods could be employed to convey transparency information to children, including notices written with child-friendly language, in-product settings and educational resources. In our view, organisations should determine which specific methods are more appropriate for them depending on the specific circumstances.

We also take note of the challenge to address the youngest audience and welcome WP29's[1] recognition that *"with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency".*

[1] The Article 29 Working Party (Art. 29 WP) was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. On 25 May 2018, it has been replaced by the European Data Protection Board (EDPB) under the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

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?

Two separate sets of notices would be undesirable, as such an approach could create a risk of confusion and information fatigue among data subjects. In addition, establishing an obligation to implement age-targeted notices in the case of services offered to both adults and children risks being interpreted as an obligation to segment the organisation's audience in a way that would contravene data minimisation requirements and the provisions of Article 11 of the GDPR.

In reality, a significant number of children today are in fact more technologically sophisticated than some adults.

Organisations should instead focus on creating notices that are clear and easy to understand for a wide audience. However, we would not rule out the creation of additional information in a variety of formats, designed for children, as an aide to improving their understanding of complicated words or concepts.

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?

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: +353 1 605 1500
fax: +353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

Children are the data subjects. As such, they are the titleholders of data protection rights, regardless of whether they are below a certain age, and they should be entitled to exercise those rights. However, that should not prevent organisations' ability to address situations where the user has known impairments or disabilities insofar as current technical and operational capabilities permit.

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 have the right and the duty to assist their children. Although there are different factors that could be considered to determine in which circumstances parents should be able to exercise data protection rights on their children's behalf, parents, children and organisations need certainty and would not be able to make a case-by-case assessment of those factors in all situations. A specific age threshold is therefore needed to ensure certainty and a consistent application of the law, in line with the principles of the GDPR.

In this respect, a reasonable threshold needs to be the age of consent, which is a limit that should already consider, and be the result of, an analysis by the relevant legislators of the different factors at play.

In circumstances where a child has an account with a service provider and is above the digital age of consent, a parent should not be able to exercise any of the rights in relation to that account to the extent that is not possible to verify that the requestor is acting on behalf of the account holder. It should be sufficient that an account holder can download their data directly and in turn provide access to others as they wish (and equivalent actions for the rest of data protection rights).

Particular consideration needs to be given to services which allow for anonymity. These services generally will not know who the user is. Therefore, it would not be practicable to allow 'parents' to obtain 'their' child's data. Such a requirement would require operational and technical solutions that don't yet exist; and may in some cases jeopardise an organisation's ability to provide the service that people come to use - furthering public discourse and even anonymity.

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?

Finding a solution that takes into consideration parents' right to protect their children and children's right to privacy when dealing with access requests is extremely difficult. Therefore, it shouldn't be for the data controller to strike any balance or make any assessment between a parent's right to protect the best interests of their child and the child's right to privacy.

Technology Ireland
Ibec

Making Ireland a global technology powerhouse

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: +353 1 605 1500
fax: +353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

Technology Ireland understands that providing clear rules for children and parents would very much contribute to striking the balance between the different rights at stake as it would help ensuring certainty and transparency. We would greatly appreciate guidance from specialised civil society groups, and particularly children's rights advocates, on the elements to take into account when striking that balance in the way that best protects children's interests.

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?

See responses to questions 3 and 4 above. Technology Ireland believes that the balancing of freedom of expression and access to information, with privacy rights is key to considerations around data erasure. In this regard, the rights of children should be considered as a primary factor, unless there are unusually strong public interest issues at play.

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 responses to questions 3 and 4 above. Technology Ireland believes that the balancing of freedom of expression and access to information, with privacy rights is key to considerations around data erasure. In this regard, the rights of children should be considered as a primary factor, unless there are unusually strong public interest issues at play.

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?

Age verification mechanisms must be appropriately balanced in view of data minimisation requirements under the GDPR. They should also be inspired by a diverse audience and avoid leading to discrimination. Users should also feel encouraged to use them without lying about their age.

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? (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?

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: +353 1 605 1500
fax: +353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

In our view, the "reasonable efforts" that need to be made for the verification of parental responsibility have to be measured and balanced with data minimisation requirements and the need to avoid excessive data collection, as expressly recognised by WP29. This balance needs to take into account the current state-of-the-art technology.

Following current industry practice, some of the methods that are used to verify parental responsibility are the verification by SMS or email code, or the verification through payment card. However, organisations should have flexibility to develop other methods and approaches as they adapt to new technologies and we would welcome regulators' collaboration to address the difficult challenges that arise to comply with parental consent obligations without detriment to other rights at stake.

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?

Assessing the issue of a change in the applicable age of consent requires an analysis of the consequences that any measures would have for the data subjects, whose interests should be the primary area of focus. Any steps must be taken with children in mind, aiming for an outcome that can benefit them from the different perspectives.

Locking users out of services may deprive data subjects of the tools they use to access information or educational resources they need for school, as well as records of prior activity —such as documents or pictures — that they may want to retain. It may also cause confusion among data subjects that now see themselves deprived of the resources that they were lawfully using prior to May 2018.

We note too that consumer rights issues come into play in this instance, for example where a child has purchased content or a device. The processing of the data in these circumstances can be based on the controller's legitimate interests.

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

Organisations have the challenge of balancing children's best interest with a way to provide scalable services, and it appears that the only reasonable way to do so to be legally compliant would be by requiring that users are at or above the age of consent established in their own country, when consent is required.

This, however, poses challenges even for the interests of children.

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: +353 1 605 1500
fax: +353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

For example, an organisation that offers their services in multiple EU countries from a single establishment and is subject to the law of the country where it's established. Is that country's age of consent the one the organisation should implement for all services rendered across the region? or should that organisation change the age of consent for users located in different countries? It would be a disadvantage both to controllers and children if a child in a country where the digital age of consent is lower than in the country were the controller is established is not allowed to use the services of that controller without parental consent. Similar questions arise when thinking about families that go on vacations or move their residency between Member States.

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 intrusiveness and sensitivity of the data needs to be fully taken into account. An ability to inform parents must also be taken into account. It should be a matter for the individual data controllers to decide whether to seek parental consent or not.

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?

This should be a matter for individual data controllers to assess taking account of whether they wish to seek parental consent for doing so.

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?

The principles of privacy by design and by default should form part of organisations' privacy programs.

In terms of the specific settings to be designed, our view is that parents should have a critical role in determining what would be appropriate for their children. Introducing the obligation to establish default settings unilaterally could create challenges, including how could organisations know what the appropriate default settings should be, whether those default settings may deprive users from accessing certain services, or how to find the right balance between the different types of families and stages of maturity.

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?

Technology Ireland
ibec

Making Ireland a global technology powerhouse

Technology Ireland
84/86 Lower Baggot Street
Dublin 2
Ireland

tel: +353 1 605 1500
fax: +353 1 638 1500
email: info@technology-ireland.ie
web: www.technology-ireland.ie

The principles of privacy by design and by default should form part of organisations' privacy programs.

In terms of the specific settings to be designed, our view is that parents should have a critical role in determining the settings that would be appropriate for their children. Introducing the obligation to establish default settings could create challenges, including how could organisations know what the appropriate default settings should be, whether those default settings may deprive users from accessing certain services, or how to find the right balance between the different types of families and stages of maturity.

Clarity is also required around what is considered to be "younger children" in this context.

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 GDPR text contains provisions relating to the processing of children's data to encourage the drawing up of codes of conduct in relation to certain issues concerning the processing of children's personal data (Articles 40 and 41). Technology Ireland believes that codes of conduct, like certification, can play an important role in facilitating, as well as demonstrating, compliance with the General Data Protection Regulation (GDPR).

Technology Ireland notes GDPR's Art. 40(1) which provides that codes should contribute to the GDPR's proper application 'taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises'.

Technology Ireland also notes the ongoing consultation on the European Data Protection Board (EDPB) Draft Guidelines on codes of conduct and monitoring bodies.

As referenced earlier in this submission, Technology Ireland would value input and guidance from specialised civil society groups, and particularly children's rights advocates, on the elements to consider when striking that balance in the way that best protects children's interests. The National Advisory Council for Online Safety (NACOS)[2] is composed of such a mix of stakeholders and may provide a suitable forum to inform this exercise.

[2] The National Advisory Council for Online Safety is a forum for non-governmental, industry, and academic stakeholders to discuss online safety issues. The Council was formed as part of the Action Plan for Online Safety 2018-2019. The Council has 20 members and a chairperson. The membership of the Council is drawn from children's and parents' organisations, major online platforms, and experts on online safety issues.