Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR

Issued 19th December 2018 by the Data Protection Commission

Three Ireland Response

5th April 2019

1. Introduction

This document is the response of Three Ireland (Three) to the Data Protection Commission's (DPCs) public consultation of 19th December 2018 on the processing of children's personal data and the rights of children as data subjects under the GDPR.

As a processor of children's data, Three welcomes the opportunity to contribute to this consultation in order to assist in the production of guidance material by the DPC in this area.

2. Response to the Questions set out in the Consultation

Q1. What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?

A. Pop-up short privacy notices or easily found and easily understood privacy notices could be used. 'Scroll over' function could be considered where explanatory words appear when the mouse arrow scrolls over text boxes where personal data is collected, explaining the need for that data.

Q2. 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?

A. Yes, separate sets of information should be made available. Privacy notices in general should be easily read but children's privacy notices should be concise and more accessible to children.

Q3. 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. A child should be able to ask for their data at any age at which they can make that request in writing. There may be an issue over verifying that the child has made the request as a child will have very little identification documentation.

Q4. 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?

A. Three considers 13 to be an appropriate age below which a parent could make a request on a child's behalf. A joint application could certainly be made lower than this e.g. age 8 up to 13.

This age could be made higher should there be other circumstances for example the mental and physical status of the child.

Q5. 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. The child's rights are paramount, and organisations must uphold those rights as if the child were an adult. Parents however as the guardians of their children must be able to advocate on behalf of their children but Data Controllers and Data Processors must always be mindful not to breach the rights of the child by assuming the parent is always using that data to protect a child's rights.

Q6. 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?

A. A child should be able to exercise their right to erasure on the same basis as an adult data subject.

Q7. 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?

A. 13 should be the upper age limit.

Q8. 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?

A. Date of birth should be requested.

Q9. (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?

A. A confirmation box should be ticked and perhaps their identity validated to avoid against a child ticking the box.

Q9 (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. Three is mindful of its duty to avoid excessive processing particularly where sensitive information might be disclosed, and of the risks around collection and storage of sensitive documents such as birth or marriage certificates and would welcome advice in this regard.

Parental responsibility can take many forms and advice on guardianship, loco parentis, disputes between joint guardians etc would be welcome.

Q10. 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?

A. Yes, where consent is the basis of the processing.

Q11. How should such online service providers ensure they comply with different ages of digital consent in different Member States?

A. Drop down boxes could be used where the child could select the flag of the country they live in and then a drop down could be used for the correct age.

Q12. 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?

A. Three submits that intent and the nature of the profiling is a vital characteristic to be considered, and that a distinction can be made between profiling which targets children knowingly, or specifically on the basis that they are children, and profiling which could potentially include children without the knowledge of the profiling party. While we support a prohibition on the former, we submit that a prohibition on the latter could place entities in the invidious position of having to either cease all profiling, or to collect additional personal data from data subject to determine their age, for the sole purpose of determining compliance with the prohibition.

Q13. 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?

A. Yes, organisations should be prohibited from profiling children for marketing purposes. However, as noted above, data controllers may not be aware of the age of subjects being profiled, or of whether the subject is a child. We propose that any prohibition be limited to profiling where the age of the child is an element of the profiling and targeting or is or should be known to the profiling party via other means.

Q14. 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?

A. Age appropriate privacy notices should be provided, and dates or years of birth requested. Privacy settings should be prominently displayed and easy to understand.

Q15. 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?

Wherever privacy settings are configurable, settings for children should default to the least permissive, so that children are always opted out of any processing until or unless they choose to positively opt in.

Not answered.

Q16. Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation?

A. This consultation discusses the rights of children concerning direct marketing. Section 30 of the Data Protection Act 2018 provides that processing for the purpose of directly marketing, profiling or micro-targeting a child, i.e. a person under 18, is a criminal offence. Three notes this section has not yet been commenced. Three requests that the consultation report provides clarity on whether it is intended to commence this section, and if so:

- When the section is likely to be commenced;
- Whether this section applies to cases where the age of the data subject or the fact of their being a child is not known;
- Whether it shall be a defence to the offence that reasonable efforts were made to ascertain the age of the subject, and if so the standard of reasonableness;
- Whether the criminal standard of proof applies to the offence.

30