Consultation by Data protection Commission

Children Exercising GDPR Rights

Submission of Department of Education and Skills

Introduction

The Department has considered the consultation documents and the questions proposed. The views set out below represent a summary taking the views of various areas of the Department into account. The Department is happy to engage further with the DPC on the issues if required.

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

- Consent forms signed by parents.
- Simple, clear and readable information, images and animation in communications material
- Include data protection information in presentations and information booklets

2. What approaches should be used by organisations whose products and 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?

- Where both audiences are targeted a dual set of information could be used.
- Specific tailored information for children in additional to information published on the website
- Use plain English and do not use different transparency information

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?

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?

- Children have a right to their own data, organisation bears the burden of delivering the data in an appropriate manner to ensure they understand and that the data does not distress them.
- In terms of education, 12 or 13 is a natural boundary age when children move to secondary education. This could be considered for a relevant point for rights to be exercised.
- However, there is a need to go beyond simply age, for example a set of criteria to assess appropriateness of releasing the data might be developed, including capacity of child to understand data, potential adverse impact on the child, the nature of the data medical/ health, etc.
- The digital age of consent could be considered as a cut off for parental rights over children's data, i.e. once 16 only child can apply. Assessing factors such as maturity are subjective therefore not advised.

- In summary:
    - Under 12 or in primary education – Parent Guardian alone can exercise rights on behalf of child
    - 12 to 16 – Child can exercise rights themselves and parent/guardian can exercise with consent of child
    - 16 or over – only child can exercise

- However for medical and similar data:
    - Up until child is 18, a joint request from age 16 for medical data(currently aged 16 can give consent to treatment except psychiatric)
    - Up until 16, or child is incapacitated, joint request not recommended but a child could sign a request sent by a parent.

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?

- In sensitive situations a child's right to their data should not be superseded by the interests of their parents/guardians.
- Once child is 12 or 13 views should be sought and considered
- Data access request should be accepted from parent up to 16 and not after unless child is incapacitated

6. At what age or in what circumstances should a child be able to make an erasure request to the organisations and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration?

- Right to erasure important but not absolute right.
- Cases by case basis, especially in terms of public services rather than private sector elective systems. Can a data subject seek to be removed from all public record etc.? This would have significant implications.
- Generally children's requests should be acceded to and also adults who gave their data when children.
- Organisation should have clear retention policy, more than age of child to be considered. Policy should explain reasons for retention, future use, balance between child's right (erase) and public interest (retain)

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 allowed 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?

- Case by case. Should be able to request erasure when the parent gave consent on behalf of the child.
- Request should be considered in context of retention policy. Beyond 18 parent should not be making request unless child is incapable of making the request. A parent should be able to on death of a child unless part of investigation. Between 16 and 18 a joint request for erasure could be considered.

8. If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could or 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 ?

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 (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 of the child? How should "reasonable efforts" be measured in this regard?

10) Prior to 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?

- Two factor authentification is needed to verify data of birth.
- Use of method of payment to verify id of parent/guardian. Example of Microsoft who request payment details when adult sets up account then provided backup e.g. e-signature or payment details for each child added to the account.
- Parental consent should apply between 13 and 16. Issue is how to verify this information.

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

12. In the case of marketing to a child, which factors should be taken into consideration when balancing an organisations own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?

N/A

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?

Marketing to children (vulnerable audience) and profiling for marketing to children is fraught with potential issues and would need to be considered carefully.

14. What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products they offer to children?

- From inception of process/system organisation must ensure processing of children's data is clear, fairly obtained, lawfully processed, minimal, clear purpose, accurate, up-to-date, minimum retention
- Redacting direct contact details of children and names of 3rd party children where appropriate – need well defined privacy statement, safe methods of electronic transfer, restriction of access to data by internal staff
- Data Minimisation and pseudonymization should be used on personal data

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 for a child? For

example, should there be stricter privacy settings for younger children? How should these variations in the privacy be given effect?

- Technical challenge but when service provider is providing service to person below age of digital consent they should safeguard and GDPR specifically mentions children's data.
- Similar privacy setting should apply to all children, 6 or 14 year old are both legally children.

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

- The document makes no reference to children with disabilities and how their rights will be safeguarded. In questions where the DPC asks if age is the only factor, children with disabilities should be considered.
- Clarification needed about what age of digital consent means and how this affects subject access rights of a child/parent on someone under 18.
- DPC should define certain terms used – i.e. meaning between "child" and "young person".
- Consultation document suggests that data subjects should be allowed to make requests for erasure if now an adult but gave the data when a child. This seems to undermine the part where everyone understands the data usage.
- DPC lesson plan needs to be age appropriate and suitable for all ages of children.
- Please expand the definition of personal data to include images and video or audio recordings and show how they can be used to identify a child
- Pitfall of digital age of consent being 16 is that sites are not compelled to have safeguards in place for younger children.