ProPrivacy Consulting Limited
Office 5, CoWork
1 Landscape Terrace
Mallow, Co. Cork
P51 T383
15 March 2019

Dear Sir/Madam

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

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

Organisations could employ video messages or pictorials to convey transparency information to children making use of relatable characters and using language that is simple and easy to understand.

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?

Organisations that aim to engage with both adults and children should have two different and separate sets of transparency information. Transparency information for children should be clear and made apparent at the outset of the use of the platform, the signposting or access to that information not be hidden in layers of text.

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?

Coming from a South African law background, we appreciate that a child between the ages of 7 and 14 has an awareness of action and consequence. To make matters simple, I believe the age of 13, but with the knowledge, not necessarily the consent, of a parent or guardian, is an appropriate age for a child to make an access request to an organisation and receive a copy of their personal data. I believe the parent or guardian should have knowledge of the request and receipt of the personal data in order to be able to deal with any fall-out or consequence of the child receiving the data and to manage any undue process together with the child. I believe age to be a somewhat artificial factor, but it is

what it is. It would be very difficult to base the request and receipt of personal data on factors such as maturity or EQ, for example. In terms of the assessing the sensitivity of the personal data to release to the child, perhaps an awareness of the emotional state of the child might be a consideration or a history of conflict such as a disciplinary record of incidences at school. Considering sensitivity, again, I revert to comment on knowledge of parent or guardian in order that they be permitted to guide and counsel the child on a response to the personal data being received.

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?

I believe that children enjoy the right to privacy, but this is tempered by and balanced against the responsibility parents or guardians might have toward the child. I would be of the opinion again that at age 13 a child should enjoy the right to privacy but understand that this is limited by the responsibility of the parent or guardian. I believe there are circumstances under which a parent or guardian could make a case for an access request without the child's knowledge. Where there is a suspicion of wrongdoing by or against the child, it would always be my counsel to have an official body involved be that the school, Tusla or the Gardaí. Having dealt with sensitive issues in the past, it does not always do well for a parent or guardian to go barrelling headlong into a suspected incident where evidence might have to be preserved or where an awareness of parental involvement might encourage a wrongdoer to go into hiding. If an official body is involved with an investigation or complain, justice might better be served. Regarding an upper age limit, obviously when the child becomes an adult with capacity, a parent should not be permitted to have access to personal data, however, the parent should still be permitted to make an access request for the personal data of the child that was processed before the child reached adulthood. Perhaps there is also room for a reverse of the above, in that a parent or guardian should have the right to make an access request when the child is aged 13 to 18 but with the knowledge, not necessarily the consent, of the child if the situation is not a sensitive case as outlined above. The child should be afforded the right to object to the access request by the parent or guardian.

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?

There might be a consideration of a parent or guardian making an access request with the 'permission' of the commission through a process whereby they identify a valid purpose for the request and be issued with a receipt which indicates lawfulness of the access request. Part of this process might be that there be an indication of sensitivity level of the situation where if the situation is not considered to be highly sensitive, proof of the child's awareness

of the access request is considered by the commission. The parent or guardian could then present the receipt from the commission to the organisation receiving the request who could then validate the receipt against an electronic register.

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?

This is a non-negotiable for me and it should be at any age without question. No child should be subject to tracking or be in a position where a profile is built up on them over time or that they become part of data stores. Furthermore, an organisation that is subject to an erasure request should be forced to make a full disclosure of any and all data shared where the child has been a part of that data set.

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?

I would temper my answer in 6 here and say that there should be reasonable grounds upon which a parent or guardian needs to rely before making a request for erasure of a child's data. I would imagine a similar process to my answer in 5 would provide a check and balance between the ages of 13 and 18.

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?

Please, dear sweet Lord above, don't go the route of the 'porn pass' in the UK. For the love of God. There are good examples of identify and age verification where a form of national ID is required (birth cert or passport), a photo to verify against the ID (which wouldn't work with a birth cert but would work with a passport), and then some platforms also ask for a short video of you saying something specific. A learner permit or moped/motorcycle licence that is issued at age 16 could be used as verification. Once your identification and 16+ status is verified, and the proof of verification is erased. In Ireland, it is not hard to solve this problem with technology where schools, churches and the Gardaí are connected to a national verification register that could allow participation of children if they wanted an online ID. In this instance, the register could issue them with an anonymous ID that is checkable. However, opening access to platforms outside of Ireland would pose a challenge. There are also security considerations and I would imagine there would be a widespread suspicion regarding tracking of the ID and tracking and profiling of people,

generally. If it is possible to solve the issue using existing systems such as vehicle licences, that would be preferable.

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?

A birth cert presented would verify status of a parent, where the parent would have to go through the same process as discussed in 8 to verify their own identity. Where an adult is a guardian and not a parent, there would be an official communication, even a letter on a government department letterhead that could be used to verify status.

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

I believe that it is not difficult to implement technological measures available to verify age and identity therefore I believe the standard to be quite high in terms of gauging effort. There has been too much window-dressing in the past by large corporations providing digital services allowing children to bypass half-hearted attempts at age verification with massive legal disclaimers to protect the corporation. The effect that social media platforms and connectivity have had on our children is coming to the fore now. There is responsibility on organisations providing access to platforms to children to take consent-related issues seriously.

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?

I don't believe that a user should be locked out of a service until they reach 16, but that a time period be set during which the child should be able to proffer the correct adult-led consent. If the child is not consented by a parent or guardian, then, their access should be suspended until they can prove an age of 16+.

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

Proof of address from a parent or guardian during the consenting process would fit in with my ideals of having a parent aware of a situation but not necessarily having to consent or condone access for the child to the platform.

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?

Marketing to children based on legitimate interest should not be permitted at all, ever. I have no comment on factors as this should not be happening. Direct marketing to children should be based on verified consent and consent alone.

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?

Yes, absolutely, organisations should be prohibited from profiling children for marketing purposes. Children are not a commodity and we should respect their right to develop their imagination without the exceptionally distressing amount of influence that is currently being exerted over their minds.

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?

There should be parent or guardian access to accounts with access to data downloads and the ability to erase the account on behalf of the child. In instances where appropriate, the verification of the permission of the DPC to act could be built in as an extra step. Accounts of children should not allow full access to platforms until age is verified. Period verification could be instituted to cut down on fraudulent access. Two versions of transparency information in the form of a detailed and full privacy notice aimed at the parent or guardian with a child-friendly version available to the child where it is explained in absolutely clear terms to the child what is happening with their data on the platform and especially where else the data goes to in order to start creating an awareness in children of the connectivity of data stores and processors. Built in bullying reporting with report now type buttons always available to children are a non-negotiable for me on platforms where interaction might occur with other users.

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?

As a default for all children, nothing should be set with public access allowed. I would be of the opinion that children younger than 13 should never be allowed to share any information publicly and then from age 13 upward, default private access. Even up to age 16, it would be my opinion that children shouldn't be permitted to share information publicly. From age 16 to 18 I would be of the opinion that information could be shared publicly but that should

never be a default setting. On this note, tagging of children in media where tagging ties a person to a piece of information or media should never be allowed for under 13s, not even with a review setting on tags. Further it is my opinion that direct messaging functionality should also not be allowed for children under 13.

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

Parents, guardians and other adults need to be aware of the violation of privacy rights of children that they are responsible for by sharing the personal data (media especially) of children on social media platforms and the future impact this sharing will have on children as they become aware of their space in society. Parents, guardians and other adults should not be in a position where they can unilaterally consent (or merely choose to) process children's data in this manner. We are not a in a position to turn a blind eye to the practices of the organisations running large social media platforms and their ulterior motives for encouraging this type of data sharing by adults.

Sincerely,

[redacted]

CEO ProPrivacy

Phone: +353 21 234 8890 Email: [redacted] Website: www.proprivacy.ie
ProPrivacy Consulting Limited (t/a ProPrivacy) CRO Reg: 628639 VAT: 3547299MH
Registered Office: Bridgetown, Castletownroche, Co. Cork