5 April 2019

Google welcomes the opportunity to provide comments on the important issues being addressed by the Data Protection Commission's public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation.

QUESTIONS FOR PUBLIC CONSULTATION

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

We will respond to questions 1 and 2 together.

There are a variety of methods that organisations can use to convey transparency information to children. What is suitable and most effective will depend on the intended audience, the nature of the services and products provided, and the specific processing being undertaken.

The presence of such a range of variables means, in our view, that organisations should be permitted to determine which methods are appropriate for their products and services. User testing with parents and children should help drive that assessment. We also believe that there is room for the development of best practice principles, but these should allow data controllers to have the flexibility to innovate and deal with different technologies and business models.

Below are examples of different methods that products or services that are directed to children (e.g., by means of their content, features, marketing, design, and intended audience) could employ to convey transparency to children:

- Notices written with child-friendly language. Providing children with a notice that reflects the key aspects of the processing using child-friendly language would be helpful to provide transparency for the child and also to assist parents to summarize and explain this information for their children.

- Product settings and in-product notices. In some cases, clear and easy-to-use product settings and in-product notices would also be a good way to address transparency and

will be more effective in conveying information than separate notices, particularly for younger audiences. Simple buttons or audio alerts help children better understand the technology they are using, which is a relevant aspect to be able to understand how their data is being processed.

- General educational resources. Educating children about technology, safety and privacy is key to achieving transparency. Children will be able to better understand notices and product settings if they have some basic knowledge about these concepts. For that reason, we invest heavily in initiatives such as our new Safety Center, which provides tools, information and resources for families in Ireland and around the world.

  We also think that appropriate education from public authorities in this space would play a key role and measures like including privacy and safety in schools' national curriculum should be encouraged.

- Promote resources from DPAs. We support data protection authorities' efforts to build educational resources in this area, such as the lesson plan on personal data created by the Data Protection Commission as part of the second stream of this public consultation, and we remain at their disposal to collaborate. If authorities were interested in collaborating with organisations to use their platforms to promote their educational resources, a good way to promote this information would be for organisations to link to some of those resources as part of the educational materials they provide.

In the case of products or services offered to both adults and children, the ideal state should be to design a privacy notice that works for everyone. Organisations should place particular emphasis on user comprehension when designing transparency notices, to take into account the broadest possible range of learning styles and abilities. However, we recognise that it may not always be possible.

Offering separate sets of transparency information risks creating confusion among data subjects but organisations should evaluate on a service-per-service basis whether additional information or help center-type of content would be required to explain difficult concepts and ideas to children. The nature of the service and processing might mean that specific explanations should be required for children of different ages or parents of children of different ages because a one-size-fits-all approach would not really work for the diversity of services that are available today. Article 29 Working Party guidelines on transparency[1] ("WP260 Guidelines") recognise this complexity when indicating 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] WP260 Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018.

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? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?

We will respond to questions 3 and 4 together.

The question of a child's ability to exercise access rights on their personal data is particularly complex. On the one hand, parents, children and organisations need clear rules that can be scaled across services and users. On the other, addressing this issue requires balancing a child's personal rights with their need for supervision and protection by a holder of parental authority. Children of different ages may have very different levels of maturity, ability, and awareness, and interpersonal dynamics may vary considerably from one family to the other.

In its WP260 Guidelines, Article 29 Working Party emphasised that "*children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies*." In our view, this means that children should be allowed to access and receive a copy of their data regardless of their age or circumstances, but always subject to the appropriate national subject access provisions, which seek to balance the rights of access with individual welfare. In addition, such access should not necessarily preclude parallel communication with a parent or exceptions to the general rule where the particular circumstances require this to ensure the best interests and welfare of the child.

The child is still the data subject, even when they are below the age of consent or have not reached full maturity. Therefore, as mentioned above, they should as a general rule be allowed to access and receive a copy of their data. At the same time, parents of children below a certain age threshold have the right and the duty to assist their children and should therefore be allowed to also exercise these rights on their behalf.

The right and duty of parents to represent their children when exercising these rights can be influenced by many other variables such as the maturity of the child, their need for privacy from their parents, specific family dynamics, social and cultural norms, and more. However, parents, children and organisations need certainty about the threshold beyond which a parent should no longer be able to request access to a child's data.

One way to address this issue in a way that balances parents and children's needs could be to rely on the age of consent as the threshold. Member States should have already considered the aforementioned factors and variables when setting their age of consent, and it would seem

reasonable for parents and children to expect that similar rules would apply to cases where similar factors and variables must be considered. Of course, as mentioned above, that does not mean that specific thresholds or rules would preclude parallel communication between parents and children, exceptions to the general rule where the particular circumstances require this, and the need for parents to always ensure the best interests and welfare of the child.

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?

We would welcome the input of child protection groups, academic experts, teachers, other practitioners working in daily contact with children, and parents and children themselves, to find the most balanced and protective approach for children in this area and to think of practices that organisations can implement across services and in a scalable manner.

In addition, the balance between the rights of parents and children may depend on the specific type of service that organisations are providing to children. A way to strike the right balance between parents' rights to protect their children and children's rights to privacy, while at the same time give flexibility for each family and child to adapt to their particular circumstances, could be to ensure that appropriate transparency measures are adopted. In our view, these measures would include providing information for children about the controls that their parents have, and setting up a clear age threshold tied to the age of consent that would make it easier for them to understand at which stage they can be more autonomous with regard to their data processing.

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? 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?

We will respond to questions 6 and 7 together.

The position should be consistent with how other rights are regulated. We need to make data subject rights frameworks understandable for children, parents and organisations. Although the assessment of this question requires a similar set of balancing factors to those discussed in questions 3 and 4, children, parents and organisations alike would benefit from some general rules. Again, the age of consent that Member States have adopted might provide an appropriate framework, in the understanding that exceptions may apply and parents must always act in the best interest of the child.

Additionally, in order to address data erasure requests, organisations need to balance privacy rights and the child's special conditions, such as impairments or disabilities, against the right to freedom of expression and information, and they should consider that in many cases the rights of children will likely outweigh other rights at stake, unless there is an unusually strong public interest.

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?

GDPR requires personal data to be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Article 5). GDPR also foresees that *"if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation*" (Article 11). We understand that any methods to verify that a child is above the age of consent should respect these data minimisation principles.

In designing appropriate mechanisms to confirm the age of users, it is important to recognise that information about age can be reliably solicited if certain steps are taken to ensure the "neutrality" of the age screening.

Age verification mechanisms should not encourage children to lie about their ages. Organisations should provide users with choices which are not restricted to ages above the age of consent (e.g., users should either freely enter day/month/year of birth, or use a drop-down menu that includes ages that are both under and over the age of consent). In addition, some technical mechanism should be implemented to prevent a child from back-buttoning and entering a different date of birth on the form after they have confirmed their age. We encourage the Data Protection Commission and other authorities to consider issuing guidance about how these mechanisms can be effectively deployed given their consistency with data protection principles.

These measures could be complemented with additional steps that organisations could take to ensure that children interacting with services are being treated appropriately while also respecting data minimisation requirements. For example, when organisations acquire actual knowledge that a user is below the age of consent, they should take action for the child's personal data to be treated consistently with data protection rules. Furthermore, to cover the reasonable cases in which adults may use services or portions of services directed to children, organisations offering these services should be able to treat their adult users as adults if they take steps that are reasonably calculated to ensure that the individual interacting with that service or portion of the service is not a child. These steps could involve prompting a neutrally

age screened individual to make an active choice to enter a PIN or other device or account credential before using a product or service considered targeted to a child, which would enable important user experiences for adults while also ensuring appropriate treatment of children.

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?

We welcome the Article 29 Working Party's recommendation for a proportionate approach[2]. Parental consent mechanisms should be guided by data minimisation principles and not lead to excessive data collection. For example, the collection of Government IDs should be restricted to exceptional circumstances and not be the rule for all cases.

We have found in user studies that parents are reluctant to provide personal information for the sole purpose of providing parental consent. Taking into consideration the available technology, when used in conjunction with a neutral age screen, methods such as sending a code via SMS to a telephone number on file or an email, verifying a user's payment card details, or requiring user authentication and checking account attributes that have been reliably correlated with parental status, could be examples of reasonable efforts to verify that a person has sufficient parental responsibility to provide consent.

Organisations should also have sufficient flexibility to implement different kinds of mechanisms that are reasonably calculated in light of available technology to meet the GDPR standard, and to evolve them as technology advances, provided they can support their approach as meeting requirements. Flexibility is also necessary for organisations to be able to implement mechanisms that will not increase the chances of excluding individuals from accessing those services and products (e.g., some parents may not have credit cards). Industry consensus and the implementation of innovative mechanisms should be encouraged.

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?

In our view, for processing that requires verifiable parental consent, it is important to balance the need for parental consent with the rights of children under 16 who lawfully accessed services prior to May 25, 2018. In many cases, they may be relying on these online service providers as their primary vehicle for access to important educational content and information. Thus, the

[2] See Article 29 Working Party Guidelines on Consent adopted on 10 April 2018.

unintended consequence of locking out users is that, for those children who may not have access to a parent, they could be deprived of not only access to the service, but access to important content and information that they have stored online such as homework assignments or other content they may have created, and communications with educators.

At-risk teens may not always have easy access to a parent to provide consent, and in the worst cases, they may in fact have relied on the online service as a means of shielding certain information from an abusive parent.

Notwithstanding this, service providers should take all reasonable and proportionate steps to facilitate the collection of verifiable parental consent in a manner that is consistent with these objectives and should in all cases ensure that they have particular regard to the purposes of the processing of the data associated with the services in this transitional period.

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

The varying ages of consent in the different Member States present a complex situation. Notwithstanding the complex legal landscape on this question, Google has taken the position that we will respect each Member State's authority in determining their children's right level of maturity and decided to adopt the policy that we considered more protective. In order to create a Google Account, users need to be at or above the age of consent established by their respective country.

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? 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?

We will respond to questions 12 and 13 together.

For its part, it is Google's policy not to engage in personalized advertising or marketing to children known to be under the applicable age of consent, and not to create advertising profiles of such users. Because of variance in the age of consent across European Member States, Google currently applies this policy to all known European users under age 16. If a business chooses to use the personal data of a child under the age of consent for personalized advertising or marketing, Google understands the GDPR and regulatory guidance to require the business to obtain the affirmative consent of the parent.

Note, however, that many users of advertising-supported services are under the age of consent, and businesses offering such services have a legitimate interest in processing such users' data for the purpose of delivering ads, measuring the performance of such advertising, and

combating fraud. Google believes such processing can be done without adverse effect on the rights and interests of children or their parents, so long as the data is not processed to personalize ads or create an advertising or marketing profile. Indeed, without such processing, it would be difficult or impossible to offer free or advertising-supported services to younger users.

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? 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?

We will respond to questions 14 and 15 together.

Organisations should incorporate the principles of privacy by design and by default as part of their privacy program. This would include implementing a different range of measures, such as ensuring that privacy is considered from the beginning of the development of products and services, training employees on these standards, and ensuring there is an appropriate privacy review.

In terms of default settings, we believe that organisations should design platforms responsibly, establishing the baseline that best responds to the combined imperatives of privacy protection, users' expectations, and product functionality, and then ensuring that users have meaningful control over their own data and settings.

Striking the right balance between the necessary limits and the educational and developmental needs of children that are fulfilled through their access to online services is extremely hard. In our view, parents should be allowed to decide what are the privacy settings that work for their children. For that purpose, organisations should ensure privacy by design and by default in relation to children by offering controls to parents that help them make privacy choices and set the digital ground rules and defaults that work best for their children. With Family Link, we provide parents with mechanisms to stay in the loop while their children explore and enjoy the internet, as parents can set and tailor digital ground rules that work for their unique family. It also includes tips for families to help parents guide their children to make smart choices when using their own devices.

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

We welcome the Data Protection Commission's efforts to encourage the industry to pursue codes of practice in relation to children's data protection and we are open to collaborate with other organisations in finding ways to address the challenging issues in this area and bolstering children's privacy.