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

Facebook welcomes the opportunity to submit comments to the Data Protection Commission's (DPC) Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR.

Children's privacy protection has been an important part of Facebook's GDPR implementation efforts. But we cannot rest; we will continue to find ways to design and offer user-friendly, privacy-protective services for teens who use Facebook. We are aware that many services besides Facebook — both offline and online services — are facing similar challenges. We therefore encourage continued multi-stakeholder engagement and collaboration in this area, and thank the DPC for their leadership in soliciting the views of a diverse array of stakeholders.

I. Children as data subjects and the exercise of their data protection rights

(A) Transparency and the right to be informed about use of personal data (Articles 12-14 GDPR)

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

- Transparency is an essential principle enshrined in the GDPR, as it empowers people to control how their personal data is collected and processed. The use of communications technologies and online services form part of the everyday lives of children, particularly between the ages of 13-18. This is why it is so critical for companies to ensure they communicate clearly about their services to children.
- As companies develop and enhance their communication to children, they must find solutions to a number of challenges:
    - Young people understand and access digital services differently than adults; they may have different expectations and favour different designs.
    - Children do not represent a homogeneous demographic group. Different age categories might have different levels of understanding complex information. Even within similar age categories, children may have differing capacities to understand information depending on their literacy level, cultural background, and education.
    - There is tension between providing the level of detail required by the GDPR (e.g. Articles 13 and 14) and informing different age groups in a simple and comprehensible manner. Over-simplifying the language might create the risk of underplaying or obscuring the companies' compliance with the GDPR.
- We believe that transparent communication with any data subjects, including children, should achieve the following objectives:

- Explain data processing and data protection rights using clear and simple language.
- Deploy the most effective methods and channels for delivering those messages. To understand which methods and channels are the most effective for this audience, companies can explore employing user testing, evaluation, and refinement based on feedback prior to wider deployment.

- We also recognise that transparency for children is a field where there is much work to be done, and considerable room for innovation:

  - **Companies should strive for more visual clarity using icons and videos to explain complex data processing**. In order to capture and hold the attention of children, it is important that information is provided in a way that is fun and attractive. Design has an essential role to play here.
    - In recognition of the need for improved design approaches across all digital services, Facebook launched the Trust, Transparency and Control Labs (TTC Labs): https://www.ttclabs.net/. TTC Labs are an open platform for sharing and innovation. They contain insights from leading experts in academia, design, and law, and present prototype designs, template services and open-source toolkits for people-centric design.
    - In February 2018 Facebook organised a Design Jam in London (https://www.ttclabs.net/event/London_Design_Jam) with the goal of brainstorming best practices to provide meaningful transparency for children. The challenge was to design innovative interfaces that recognise children as sophisticated digital users and enable them to have more granular control over their data use.
  - **Companies should draft language that's meaningful to children.** It can be challenging to balance legal requirements to include certain types of information and legal phrasing on one hand, with language that's accessible and clear to children on the other. We will continue to devote resources to finding the right balance, and would also welcome guidance from regulators on the type of data protection vocabulary that is appropriate for children.
    - Facebook was ranked in the top two in a recent study by TIME and the Centre for Plain Language (http://time.com/3986016/google-facebook-twitter-privacy-policies/) examining the best privacy policies, underscoring our efforts to communicate requirements in plain and simple language to children. However, we acknowledge that this is an area were constant improvement and innovation are needed, and we are committed to working with all relevant stakeholders.
  - **Companies must also strive for transparency in offline contexts.**
    - Specific messaging within online services could be supplemented by wider media campaigns or information provided to schools and other youth organisations about data protection as it relates to children. This could be done by the organisation itself or in collaboration with regulators, government, NGOs or industry groups. Delivery of such messaging can be done through social media, conventional media campaigns, or as part of the school curriculum. Media which could be used to educate children on safe use of the internet include video clips, animations, flyers and posters.

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?

- When companies provide information to both adults and children, they must decide whether to create different versions of a document — one for children and one for adults. Unfortunately, creating two different versions could risk legal uncertainty as to the exact interpretation of the terms used. The majority of companies have created only one version of their terms of service or privacy policies, rather than a separate version for children. To date, Facebook has provided information to all users in a unified manner in order to avoid confusion and ensure consistency. We are looking forward to continued dialogue on how to provide appropriate information to different age groups, including adults and children, in a way that is meaningful and does not put organisations or users at risk of uncertainty.

(B) Right of access (Article 15 GDPR)

Questions 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?

- We believe children should generally be able to exercise their privacy rights autonomously at least with regard to online services like Facebook.
- Through the Access Your Information tool, we have made it straightforward for all people on Facebook to access their information and information about them.
- We also offer an email alias (datarequests@support.facebook.com) that minors can use to contact our specialist team directly to submit their access request.

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?

- The approach may vary by sector, and may depend on national laws. In the context of Facebook's services where children are 13 or older, we believe the child should retain the sole ability to exercise her or his privacy rights. Consistent with Article 16 of the UN Convention on the Rights of the Child ("No child shall be subjected to arbitrary or unlawful interference with his or her privacy [...] or correspondence," https://www.unicef.org.uk/what-we-do/un-convention-child-rights/), children's private communications and activity on the Internet should only be accessible upon request of the child.
- However, in exceptional circumstances - where the safety of the child is potentially at risk - the right to access private content may be extended to a 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?

- As indicated above, we believe that when the safety of the child is potentially at risk, the right to access private content may be extended to a parent or guardian.

(C) Right to erasure ("Right to be forgotten" – Article 17 GDPR)

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?

- Children should be able to exercise their GDPR data subject rights, including the right to erasure.
- In the context of Facebook's services where children are 13 or older, and consistent with Article 16 of the UN Convention on the Rights of the Child, a child is able to make an erasure request by herself or himself.
- We have made it easy for users to delete the personal content they have posted historically as they continue to grow and evolve as individuals. As part of our GDPR preparations, we also improved our Settings tab so users can more easily view and edit or delete the content they've posted.
- Where parents believe Facebook content should be deleted, particularly where this relates to photos and videos which violate Facebook's Community Standards, they can report content that has been posted by someone else and have it erased if their child in the photo or video is under 13 by filling out this form (https://www.facebook.com/help/contact/144059062408922)Where the child is over 13, we encourage the parent and child to work together to submit a request using this form (https://www.facebook.com/help/contact/144059062408922). Photos or videos involving anyone else (other than the child) will need to be reported by the relevant individual. We also take into consideration when a reported photo or video involves potential violations of a minor's privacy and, on balance, are more likely to remove in these circumstances where a minor is involved.
- In any event, all Facebook users can delete information they've uploaded or shared on Facebook at any time in their Activity Log on a per item basis, and the design of our platform makes it easy for users to do so.

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?

- The approach may vary by sector, and may depend on national laws. In the context of Facebook's services where children are 13 or older, we believe they should retain the sole ability to exercise their privacy rights.
- In any event, as explained above, all Facebook users can delete information they've uploaded or shared on Facebook at any time in their Activity Log on a per item basis, and the design of our platform makes this easy for users to do so. In addition parents can report on behalf of their children up to the age of 18 (we ask that the parent/guardian to provide proof of guardianship) by filling out this form (https://www.facebook.com/help/contact/144059062408922). Facebook users aged 13-18 can also submit themselves a request via this form (https://www.facebook.com/help/contact/144059062408922) on their own behalf.

- Generally, we do not close or disable accounts of users between 13 and 18 because a parent has requested it.
- Parents or family members may ask us to remove an account if the person is physically or mentally incapacitated. We also work with safety partners who may be able to frame sensitive family situations and for us to provide support to a family in distress.

II. Safeguards

(A) Age verification (Article 8 GDPR)

Question 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?

We appreciate the underlying goal of ensuring children only access services when they reach the appropriate age. There are a number of important considerations to resolve in this area, including:

- **Data minimisation:** Verifying a data subject's age could lead to collecting more information than needed for the provision of the services, and also from many people outside of the relevant age bucket of 13-18, which would go against the GDPR principle of data minimisation. Traditional age verification methods involve, for instance, requesting documents from individuals in order to verify their identity (e.g. ID, birth certificate and passport), as well as other information such as credit card numbers and telephone numbers. In the case of many online services, this type of information would not be originally required for the provision of the service.
- **Scope:** Age verification would, theoretically, require every data subject to have her/his age verified before using services that are subject to Article 8 of the GDPR. In other words, using the methods described above, adults also would have to submit proof of age since services wouldn't necessarily-- upon registration-- be able to distinguish between children who are falsifying their age and adults who are reporting their accurate age.
- **Size of the organisations:** Age verification would likely have a strong impact on smaller apps and services that have fewer human and technical resources.
- **Data retention:** It is also unclear for how long companies would need to or be required to retain the additional personal data contained in ID documents.

- **Legal requirements:** The GDPR does not explicitly require controllers and processors to verify the age of data subjects, even where they rely on consent as a legal basis for the processing. Rather, the GDPR requires controllers and processors to make reasonable efforts to verify that parental consent or authorisation have been given.

At Facebook, we require people to provide their birthday upon registration and employ measures to (1) prevent under 13s from signing up for Facebook and (2) detect underage users who were able to sign up.

- When users sign up to our services, they are required to enter their date of birth. If the user provides a date of birth under the age of 13, we do not allow them to sign up. We present them with a general error message rather than an explanation that their date of

birth was the reason for being blocked from registering. This message also directs users to our community support team. This is intended to make it harder for them to circumvent our policy and system.

- We also ask people to report underage accounts, and we provide a specific form for this (https://www.facebook.com/help/contact/209046679279097), which be populated by both users and non-users of Facebook services.
- We ask our internal reviewers who are reviewing an account for other types of violations to also report whether they believe that the account belongs to someone under age of 13.
- We delete the accounts of children under 13 as soon as we become aware of them: once someone is reported for being underage, they are being "logged out" and will only be able to access their account again when they prove they are 13 or older by submitting an ID.

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?

- We recognise the need for a multi-stakeholder discussion in relation to this point. We welcome initiatives of DPAs, such as this consultation, to prompt this discussion.
- It is very difficult for companies to determine who is the legal holder of parental responsibility and when they can exercise their parental authority vis-a-vis their children in the data protection context. This is why Article 8 of the GDPR calls for data controllers to use "reasonable efforts" to verify that consent is given or authorised by the holder of parental responsibility over the child.
- First, legal provisions around the exercise of parental responsibility vary across EU member states — for example, some member states would require both parents to authorise their child's consent, whereas in other member states only one parent would need to authorise consent. Second, it would not be practical for companies to collect or authenticate legal documents confirming which individuals are, in fact, holders of parental responsibility for a specific child.
- As one option, organisations could ask the person providing consent or authorisation on behalf of the child to confirm whether they have parental responsibility by answering "Yes"/"No" to the question "Do you have parental responsibility?". While a lightweight action, at a minimum this could help bring awareness to the issue and provide some friction to ensure the true holder of parental responsibility authorises consent.
- At Facebook, we have designed a GDPR-compliant consent process for teens and parents that is easy and streamlined, and which discourages misuse. We give children the opportunity to consent to two different things: (1) seeing ads based on data from partners and (2) including religious and political views or "interested in" on their profiles. If children consent to either or both of these, they must ask their parents to authorise their consent.
    - If the parent/guardian are Facebook users, we will be able to identify them via the Facebook service. We will show them a blocking notification asking whether they are the child's parent/guardian. Children can only change the name of their parent/guardian in the platform if Facebook already sent an authorisation request to the original parent/guardian and she has not responded. Children are not allowed to designate a difference Facebook user as parent/guardian in case the original parent/guardian declined the authorisation.

- If the parent/guardian is not on Facebook, children will be able to provide their parent/guardian's email address. We will send them an email asking them to confirm whether they are the child's parent/guardian. We will also ask them to review their child's data choices and decline or approve their selection.

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?

- What constitutes a "reasonable effort" will vary on the basis of the service provided and the type of data processing that the consent is meant to authorise. As noted above, multi-stakeholder discussions around this issue are an essential next step to make sure that industry and regulators are aligned.

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?

- Information society services have long been an essential part of children's lives and help children, for instance, to (1) express themselves, (2) obtain support which otherwise they wouldn't have obtained at home or school, (3) connect with friends and communities, (4) develop social and political engagement skills, (5) obtain education and information. There are numerous examples of children who have excelled, obtained support, or raised issues via the Internet which otherwise wouldn't have happened, such as recent youth activism on climate change.
- In terms of GDPR requirements, it's important to recall that Article 8 concerns processing children's data where that processing is based on consent— therefore, unless a service only relies on consent as a legal basis for the entirety of its processing, there should be no legal barrier to allowing under 16s to continue using that service.
- The UK Information Commissioners' Office has clearly recognised the plurality of legal bases available to process children's data in their Children and GDPR guidance (https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf).
- Regardless of the legal basis relied upon, controllers and processors have a legal and ethical responsibility to protect children using their online services. As part of Facebook's approach to GDPR compliance, children in certain countries aged 13-15 (where the age of digital consent is set at 14, 15 or 16) are not be able to use the most personalised version of Facebook unless their parent or guardian has authorised their consent. We believe that adopting protective measures is a way to enable children to benefit from the use of information society services in a safe manner, without having to adopt extreme measures such as blocking or excluding them from these services until they reach age 16.
    - This less-personalised version of Facebook limits profile field options to hometown, school and gender only— there is no option to add religious views, political views, or "interested in."
    - It also prevents Facebook from using information from partners (third parties) to show ads to children.
    - In this version, children will only see ads based on the categories of age, gender and location. We don't use targeting interests or categories to personalise ads for

these children. In addition, when advertisers create ads in our system, the default minimum age to select is set at 18, so an advertiser would have to explicitly choose to target users between 13-17.
    - Children are only able to switch to a more personalised experience with permission from a parent or guardian.
    - The facial recognition feature is not available to users under age 18.

(B) Online service providers and different national ages of digital consent in the EU (Article 8 GDPR)

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

- Whenever organisations rely on consent for the processing of children's personal data, there are technological measures they can take to comply with the various age of consent requirements set out in national laws of EU Member States.
- At Facebook, we apply different age thresholds on a territorial basis across the EU.

III. Profiling and marketing activities concerning children (Articles 21-22 GDPR)

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 GDPR allows organisations to undertake direct marketing (Article 21(2)), as long as "the data subject shall have the right to object at any time to processing of personal data concerning him or her for [direct] marketing, which includes profiling to the extent that it is related to such direct marketing."
- Companies should make it easy and simple for children to exercise their right to object to direct marketing.
- The majority of Facebook's advertising does not constitute direct marketing, but we provide ways for users of all ages— including a special form for minors— to exercise their right to object.
    - If a user wishes to stop receiving emails or other communications from Facebook, she can change her preferences in her Notifications settings: https://www.facebook.com/settings?tab=notifications
    - A user may also use our objection form, found here: https://www.facebook.com/help/contact/367438723733209. Our objection form will automatically show a version that's suited for minors if you are logged in and your age on Facebook is lower than 18. If you are logged out, you can select the version for minors.

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?

- The GDPR allows profiling to be undertaken, subject to the same fundamental protections applicable to all data processing under the GDPR as laid out in Articles 5 and 6, including transparency, data minimisation, and using an appropriate legal basis.
- At Facebook, we implement a series of measures to protect children in the context of advertising. For instance, we only allow third party data from Facebook partners, like advertisers, to be used to personalise advertisements when the children or the holder of parental responsibility has authorised the child's consent where the child is under the applicable age of digital consent. We also have strict advertising policies (https://www.facebook.com/policies/ads/), particularly around regulated goods: we do not show ads related to alcohol, health supplements, tobacco and other topics such as gambling, dating, subscription services, and more to people under 18. Every advert is reviewed before it is shown. When advertisers create ads in our system, the default minimum age to select is set at 18, so an advertiser would have to explicitly choose to target users between 13-17.
- We hear and understand concerns about ensuring advertising is appropriate for children. We recognise the importance of continuing to work with industry and regulators to determine how to better safeguard children's interests and provide specific protections to them in the context of marketing, and we are ready to engage in these important discussions.

IV. Data protection by design and by default (Article 25 GDPR)

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?

- Privacy-protective default settings are a key way to provide special protections to children's personal data and children's safety online. Organisations should incorporate the principles of data protection by design and by default at early stages of the development their products and services, in particular when these are offered to children. Key considerations include whether children might need simpler explanations to understand their own choices, and how to apply data minimisation in relation to the collection of children's data.
- As mentioned previously, at Facebook we have applied by default settings to children's accounts designed to keep them safe (see below for more details). For example, children are not permitted to make 'public' posts without going through an education. Facial recognition feature is not made available for under 18.
- We look forward to further debate between industry, civil society and regulators, as well as regulatory guidance, on other measures that could be applied to incorporate the principles by design and by default to online services offered 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?

- Built in default privacy settings should be available in particular to children. For example; at Facebook:

    - When a child joins Facebook, they are automatically defaulted to share with ‘friends’ only. We provide specific education about what it means to share publicly before allowing children to post publicly.
    - We have designed many of our features to remind teens who they are sharing with, and to limit interactions with strangers.
    - Messages sent to minors from adults who they are not socially connected with are filtered out of the minor’s inbox.
    - Children's profiles cannot be found on search engines off Facebook because we prohibit them from being indexed.
    - We don’t show search results based on children's specific profile data (secondary school, birthday/age, and hometown, or current city) to adults who are not connected to the children.
    - The tool for controlling which posts other people can tag you in is switched on by default for children.
    - Because it's particularly important for young people to think before they share their location, location sharing is turned off for them by default. When a minor turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.
- Moreover, as mentioned earlier we are looking to explore options regarding a 'Privacy Check-up' that reminds users to check their current and past privacy settings by using posts as an example. This would work to encourage users to visit their privacy settings on a regular basis and change them as appropriate.

V. General

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 are grateful to the DPC for initiating this consultation and we look forward to working collaboratively on the topic of how to best protect children in the context of information society services.