Facebook Ireland Response to the DPC's Public Consultation on the draft guidance "*Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*"

I. Introduction

Facebook Ireland welcomes the opportunity to respond to the Irish Data Protection Commission's ("DPC") draft guidance, "*Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*" (the "Fundamentals"). Protecting all users, and particularly young people, is of paramount importance to Facebook. We fully support initiatives that promote a balanced approach to children's data protection in light of children's other fundamental rights and freedoms.

Our submission highlights Facebook Ireland's approach to and ongoing investments in designing online experiences that serve the best interests of our young users, and offers suggestions on aspects of the guidance where additional clarification would be useful to assist with their interpretation and application.

Summary of Recommendations:

1. We encourage the DPC to apply a risk-based approach more consistently across all of the provisions in the Fundamentals, aligned with the approaches in both the GDPR and the UK's Age Appropriate Design Code.
2. In applying the "best interests of the child" to specific areas of guidance, the DPC should emphasise the need for a holistic consideration of the standard, including a balance of the right to privacy with young people's rights to identity, to play, and to education, as well as their freedom of expression, freedom of association, and freedom to seek, receive and impart information.
3. We request that the DPC clarifies that Article 6(1)(f) GDPR may apply as a legal basis for the processing of children's personal data and specifically provide guidance on a more balanced approach to the interplay between the child's right to privacy and the exercise of other fundamental rights and freedoms of children and other legitimate interests.
4. We encourage the DPC to clarify that age verification should be viewed not as a single tactic, but rather as part of a collection of ongoing efforts that work dynamically to provide effective solutions. We further encourage the DPC to emphasise the importance of collaboration among industry and policymakers, involving children and parents.
5. With respect to profiling, we suggest the DPC tailor its guidance to focus on safeguards that are designed to prevent concrete risks of harm to young people while enabling beneficial uses of personalisation that are core to providing rich and age-appropriate user experiences.

II. Facebook Ireland's Approach: Designing for the Best Interests of Young People

We welcome the DPC's guidance to "*ensure the highest level of adherence to data protection principles, bearing in mind the obligation to act in the best interests of child users.*"[1] Centering the "best interests of the child" standard across all considerations ensures an appropriate balance between protecting young people's privacy, safety, and wellbeing and empowering them with tools to express themselves, access information, and build community online.

The following overarching themes guide our approach to designing age-appropriate experiences that serve the best interests of our youngest users:

Empowerment: Teens come to Instagram and Facebook to express themselves, to keep up with their families and best friends, to find new passions and interests, and to follow the creators and celebrities they admire. These services provide opportunities for teens to organise around things they care about, support underrepresented voices and push for societal change. They are the place where teens explore their identities and find people they identify with. We strongly believe in the importance of responsibly empowering young people to enjoy the many benefits our platform provides.

Age-Appropriate Safeguards: We appreciate that younger users require additional safeguards for their safety, privacy, and wellbeing. Our approach is expansive:

- We regularly release new features to further protect young people - for example, we recently changed Instagram's direct messaging feature to no longer allow adults to message a teen that doesn't follow them.
- We routinely make fundamental changes to Instagram to keep it a fun, low pressure place for teens to express themselves. For example, we are testing hiding users' like counts globally so teens don't have to worry about not getting "enough" likes in front of their friends. We also give people the option to set a timer on their Instagram usage so they can step away when it feels right.
- We have invested heavily in training artificial intelligence (AI) to identify content that exploits young people and children - from inappropriate interactions between adults and young people to child exploitative imagery.
- We have tens of thousands of content reviewers who prioritise reviewing and removing content that concerns the safety of children.
- We encourage teens on Instagram to make their accounts private, and provide a less personalised experience for people between the ages of 13 and 15 depending on the age of digital consent in different EU countries.
- We hire specialists in child safety and exploitation, and partner closely with organisations like NCMEC and Polaris, as well as law enforcement.

Innovation: Data-driven technologies help us keep young people safe and are essential to solving the defining challenges for our industry when it comes to protecting young people online.

[1] Fundamentals, page 59 (emphasis added).

For example, we're working on innovative ways to verify age. Verifying age will not be a single-step process, and we are investing in different technologies and systems to help us identify age - including using machine learning to understand people's ages. We also use machine learning to help us proactively find and remove harmful suicide and self-harm content.

External collaboration is also foundational to our efforts in supporting innovative solutions for protecting and empowering young people online. For example:

- **TTC Labs Youth Design Guide**: For over three years, the Trust, Transparency and Control Labs (TTC Labs), a co-creation lab that advances the user experience around data, has involved over 125 organisations globally on a major effort focused on designing for the best interests of the child online. Following extensive external consultation and collaboration with policymakers, industry, academia, civil society and young people, TTC Labs has recently published version 2 of its guide "*How to design with trust, transparency and control for young people: exploring privacy and safety through co-creation*".[2]

- **Better Internet for Kids**: We signed on to the Better Internet for Kids pledge, which was presented by youth ambassadors, developed through co-creation, and aimed at ensuring that online services are designed in an age-appropriate way. Engaging with young people in the development process is critical to defining solutions that work in practice, and soliciting and internalising their views is a central part of our approach to building for young people.

- **Get Digital**: Designed in partnership with academic experts, Get Digital is Facebook's digital literacy program that provides educational resources to help young people develop skills needed to navigate and thrive in today's complex digital world.

III. Recommendations for the Fundamentals

Facebook welcomes the centrality of the "best interests of the child" standard to the Fundamentals and the DPC's emphasis on the need for a risk-based approach in certain provisions. We note that these themes are shared across other frameworks for youth protections, such as the UK's Age-Appropriate Design Code. Adopting principles-based approaches that are consistent across different jurisdictions is necessary to enable effective and scalable technology-driven solutions to protect young people online. We offer below two overarching recommendations to support further consistency with the broader children's rights and data protection landscape, as well as specific suggestions with respect to age verification and profiling guidance.

A. Best Interests of the Child

[2] TTC Labs, *How to design with trust, transparency and control for young people*, available at https://www.ttclabs.net/insight/how-to-design-with-trust-transparency-and-control-for-young-people.

The best interests of the child principle is an important lens through which to view and balance the different rights conferred upon children under the UNCRC, which include but are not limited to the right to privacy. As outlined above, Facebook Ireland designs our services to ensure young people continue to enjoy the value they receive from our services while providing age-appropriate safety and privacy protections to protect against potential risks without unduly burdening their other fundamental rights. We caution against a rigid interpretation of the best interests standard as always meaning the right to privacy prevails against other interests and rights of the child (and by extension always against the interests of companies providing them with services) when applying the GDPR in the context of the processing of children's personal data.

As noted in the Fundamentals, applying this standard requires consideration of young people's right to identity;[3] freedom of association;[4] freedom of expression, including the freedom to seek, receive and impart information;[5] the right to education,[6] and the right to play and take part in a wide range of activities.[7] In order to protect young people's privacy without compromising their other rights and freedoms (as well as their general wellbeing), it is important that these considerations are part of a detailed balancing test to avoid unintended consequences. A holistic balancing test is relevant irrespective of the applicable GDPR legal basis for the particular processing activity and whether it is connected to commercial purposes or otherwise.

We note that different parts of the Fundamentals appear to suggest a more rigid approach than intended or applied by other regulators in similar contexts.[8] The DPC's stated standard suggests that there is no balancing exercise to be done in the event of any conflict between the child's right to privacy and all other interests and rights of the child. Given that such commercial interests would include providing the service to younger users, allowing them to exercise other rights like freedom of expression and association, it is difficult to reconcile an overly stringent approach to applying this standard with the DPC's position that children shouldn't be deprived from the rich user experience due to the principles contained in the Fundamentals. Accordingly,

[3] UN Convention on the Rights of the Child, Article 8.
[4] UN Convention on the Rights of the Child, Article 15.
[5] UN Convention on the Rights of the Child, Article 13.
[6] UN Convention on the Rights of the Child, Article 28.
[7] UN Convention on the Rights of the Child, Article 31.
[8] The UNCRC and the Charter of Fundamental Rights of the EU both recognise that the best interests of the child should be afforded "primary" consideration. The UK Information Commissioner's Office's ("ICO") Age Appropriate Design Code ("AADC"), which the DPC notes in the Fundamentals is "entirely consistent" and "in particular it is clear that the best interests of the child principle underpin both" (page 3), takes the more balanced approach by recognizing that the best interests standard must be afforded "primary" consideration (page 7). The ICO expresses the view in the AADC that, while it is true that "[i]t is unlikely . . . that the commercial interests of an organisation will outweigh a child's right to privacy" altogether, "[t]he placing of the best interests of the child as a 'primary consideration' recognises that the best interests of the child have to be balanced against other interests" and "[t]aking account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests" (pages 24, 26). Indeed, "[y]our commercial interests may not be incompatible with the best interests of the child, but you need to account for the best interests of the child as a primary consideration where any conflict arises" (page 26).

we request that the Fundamentals be clarified to reflect that the best interests of the child principle is a flexible and balanced concept.

For similar reasons, we also suggest that the DPC emphasise the importance of applying a risk-based approach across all aspects of its guidance. Such an approach is critical to preventing potential downsides of certain types of data processing for young people while still enabling them to enjoy the benefits of modern, data-driven services. This would ensure that the "best interests of the child" standard is appropriately applied in all respects.

Recommendations:

1. *We recommend that the DPC applies a holistic view of the "best interests of the child" standard in assessing the appropriateness of specific practices to which its guidelines would apply.*
2. *We suggest that the DPC clarify the importance of applying a risk-based approach across all aspects of its guidance.*

B. Legal Bases

We welcome the reiteration from the DPC that, as stated in the GDPR, all legal bases are equal to each other thereunder. In particular, we welcome the DPC's confirmation that the threshold for satisfying the vital interest legal basis will generally be lower where the processing of children's personal data is concerned, because what is considered necessary to protect the vital interests of a child may be different to what is considered necessary to protect the vital interests of an adult.

However, we query the DPC's approach to legitimate interests as a legal basis for processing children's data. The Fundamentals provide that: "*Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict with or negatively impact, at any level, the best interests of the child*."[9] This "*zero-interference*" principle goes further than the legitimate interests balancing exercise under the GDPR, and appears to suggest that no organisation's legitimate interest (or any other competing interest) can prevail when children's data are processed. Further, this "zero-interference" principle negates the possibility of this legal basis being available even if the "interference, conflict or negative impact" resulting from the processing are mitigated[10], such as by security measures.

We would respectfully suggest that the absolute principle that seems to be envisaged by the Fundamentals (i.e. no impact "at any level" / "zero interference") is inconsistent with the best interests of the child principle, the GDPR, and the approach adopted by other regulators like the ICO in its Age Appropriate Design Code.

[9] Fundamentals, page 13 (emphasis added).
[10] Fundamentals, page 24 ("In circumstances where there is any level of interference with the best interests of the child, this legal basis will not be available for the processing of children's personal data.").

As noted above, the best interests of the child principle requires a holistic assessment of the facts and circumstances. It is possible that certain processing (such as to enable communication or to ensure the security of a platform) may impact, in a proportionate way, on a children's privacy rights but may be required to enable or facilitate activities that are, on balance, in the interest of the child (such as enabling children to communicate with their peers or to protect them from potential harm). The very strict wording adopted by the Fundamentals seems to suggest that such balancing is impermissible.

Recommendation: *We ask that the IDPC clarifies that legitimate interests may apply as a legal basis for the processing of children's personal data, and specifically provides guidance on a more balanced approach to the interplay between the best interests of the child and the exercise of other fundamental rights and freedoms of children and other competing legitimate interests.*

C. Age Verification

At Facebook, we take a continuous, multi-layered approach to understanding and refining the accuracy of the age of our users. Effectively verifying age should not focus on a single-step process, but rather a collection of ongoing efforts that work dynamically to provide effective solutions. We have invested in a suite of tools to meet this objective and are committed to developing additional technology-driven solutions - including using machine learning - to increase our confidence about people's ages.

However, closer industry collaboration is also critical to developing effective and scalable measures to ensure young people consistently receive age-appropriate experiences across the online ecosystem. We believe strongly that providers across our industry must come together with governments and experts to arrive at thoughtful solutions designed with the best interests of young people top of mind.

Our Approach

Our multi-layered approach starts with requiring users to provide their date of birth when they register new accounts. This is done through an age-neutral process with technical restrictions to make it harder for users to provide false information. We also allow anyone - whether they use our services or not - to report suspected underage users on Instagram and Facebook. We have dedicated channels where we review these accounts based on these or other reports. While this approach has been appropriate in light of industry standards to date, we continue to invest in new solutions that provide ongoing age assurances.

We continue to develop and refine AI tools to identify users under 18. These tools add another layer of confidence to user-stated ages, allowing us to provide age-appropriate experiences, including by: blocking adult-only features (e.g., FB Dating); or, on Instagram, restricting messaging between teens and adults they don't know, presenting teens with the opportunity to make their accounts private (as well as providing education around what that means for the user), and making it more difficult for adults to find and follow teens. We welcome the DPC's

recognition that age verification measures can be used to provide a "child-friendly" version of a service by offering enhanced data protections for those users,[11] which is our overall aim in developing these tools.

While useful, AI tools may not always be the most appropriate measure for all use cases. Consistent with the "best interests of the child" standard, age verification solutions must support children's right to autonomy, as well as not unduly restrict their other fundamental rights and freedoms. Inaccurate AI predictions could undermine people's ability to use services, for example by blocking them from an app or feature based on false information that the person is below the relevant minimum age.

One of the greatest challenges our industry faces is ensuring that users below the minimum age do not gain access to services that are not designed for them. Parents should not have to choose between allowing their children on apps that weren't designed for them or restricting their access to apps entirely. While the issue of children under 13 misrepresenting their age will continue to be an industry-wide problem, apps designed specifically for kids can give parents more control over options and reduce the incentive for kids to be dishonest about their age. The DPC notes that compliance with the Fundamentals should "in no way justify the 'locking out' of children from a rich user experience."[12]

We are committed to continuing discussions with policymakers, experts, and families to ensure the experiences we build for our youngest users provide joy and value while ensuring their unique needs are met.

Recommendations:

1. *We suggest revising the guidelines to clarify that age verification should be viewed not as a single-step process, but rather as a collection of ongoing efforts that work dynamically to provide effective solutions.*

It is important to evaluate the effectiveness of age verification holistically, based on the outcomes resulting from a range of measures applied across different points in the user experience. This enables services to achieve the necessary level of confidence proportionate to the risks presented in a particular use case, while applying a floor of protections to users for whom we have lower confidence levels in the accuracy of their age.

In contrast, focusing on a single-point mechanism to verify age is not in the best interests of young people or an effective solution to achieve desired outcomes. First, this would require excessive collection of sensitive data like identity documentation. Second, no age verification measure is foolproof. A system built to rely on a single line of defense rather than multiple measures working in concert is less likely to be effective in the absence of overly burdensome user experiences such as upfront ID collection. In light of the need to respect data protection

[11] Fundamentals, page 40.
[12] Fundamentals, page 42.

principles - particularly data minimisation - this level of strict age verification should be reserved for areas posing the greatest risk (e.g., highly regulated sectors like tobacco and alcohol sales).

2. *We encourage the DPC to further emphasise the need for collaboration among industry and policymakers to develop age verification solutions which are consistent with data protection principles and designed with the best interests of young people in mind.*

While we strongly believe in the effectiveness of a continuous, multi-layered approach to verifying age, we also believe that these measures should not end with an individual app or website. Closer industry collaboration and investment in ecosystem-wide solutions are needed to supplement app-level efforts and ensure greater consistency in the age-based protections a user receives across their online journey. The DPC notes that it is "ultimately for industry to continue to innovate in this area," and we are committed to advancing the development of technology-driven solutions for verifying user age.

Further discussion between industry, policymakers, and the involvement of children and parents is needed to build consensus and develop technical standards for implementing this in an effective and privacy-protective way. There are a range of considerations that would need to be addressed - for example, the need for data minimisation and preventing risk of abuse by bad actors. With the DPC's support for ongoing collaboration, there are opportunities for Facebook and other app providers to design and test ideas. We remain committed to innovating in this area.

D. Profiling

We support the overall objective of the Fundamentals to protect young people from potentially harmful data processing activities. However, to achieve this goal, it must be acknowledged that all profiling is not contrary to the best interests of the child. Indeed, we are concerned that the current guidance on profiling is overly restrictive and not consistent with the risk-based methodology inherent in the GDPR. This may result in the unintended consequence of reducing the quality of otherwise age-appropriate online services for young users, contrary to other aspects of the DPC's guidance. Moreover, it is important to recognise the benefits of "profiling"-based tools in providing age-appropriate experiences for young people and enhancing safety protections for these users.

Our Approach

We have adopted a risk-based approach to personalisation that enables young people to enjoy the benefits of these services while avoiding potential harm that may be posed to those users by certain types of data processing as explained above, including the following:

- We have strict advertising policies in place for all users, including young people. Among other things, the Advertising Policies[13] and Branded Content Policies[14] strictly prohibit

[13] Facebook Advertising Policies: https://it-it.facebook.com/policies/ads/.
[14] Facebook Branded Content Policies: https://it-it.facebook.com/policies/brandedcontent.

ads promoting the sale or use of certain types of products, such as tobacco and related products, drugs and drug-related products, and adult content.

- In addition, our policies include additional age restrictions to prevent people under 18 from being shown ads for certain products or services, like alcohol, dating services, gambling, and weight loss products.
- Our Community Standards and Community Guidelines prohibit harmful content for all users, including young people. This includes content that has been identified by different regulations or experts as particularly harmful for young people, such as content depicting nudity and sexual activity, sexual solicitation, violent and graphic content, and hate speech.
- For users under the age of digital consent[15] in the EU who have not obtained parental approval, we limit the categories that advertisers may target against and don't use data that advertisers and other partners provide to Facebook about activity of those users off Facebook products to show relevant ads.

Recommendation: *We encourage the DPC to pursue a risk-based approach to assessing the appropriateness of profiling for young people and we urge the DPC to clarify the scope of activities to which these restrictions apply*.

We suggest the DPC focus on profiling purposes that are likely to cause concrete harms to children, as the draft Fundamentals' "prohibition on profiling[16]" currently encompasses all profiling[17]. It is important to target potential harms directly linked to specific profiling activities without imposing disproportionate restrictions on the many positive applications of data-driven personalisation, such as ensuring that a user sees content that is interesting and relevant to them when using a social media service.

Many modern Internet services and products are, at their core, personalised in nature. As the UK's Age Appropriate Design Code recognised in its standard on profiling, this type of processing may be "essential to the provision of the core service that the child has requested" and that turning off profiling would not be appropriate. Personalisation is an essential part of how Facebook Ireland ensures that users have meaningful experiences and see the content that matters to them. And this personalisation does not operate in a vacuum: it is accompanied by the protections explained in Section II to address potential harms. The combination of personalisation and the above-mentioned safeguards ensures that the experience is enjoyable and age appropriate. Further, profiling is also critical in conducting integrity and safety activities that are essential to reduce harmful content being accessible to users in general, including

[15] Note that this is not because we necessarily otherwise rely on consent as the legal basis for such targeting, but because (as recognised on page 39 of the Fundamentals) "[t]he age of digital consent is also a marker for online services to consider the nature and design of their services, and how to make them age appropriate".
[16] Fundamentals, page 7 ("12. PROHIBITION ON PROFILING: Online service providers should not profile children and/ or carry out automated decision making in relation to children, or otherwise use their personal data, for marketing/ advertising purposes due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so.").
[17] Fundamentals, page 51 ("Profiling is a way of using someone's personal data to predict or analyse characteristics of that person, such as services they will be interested in, their likes or dislikes, preferences, views or opinions, or their behaviour").

children. For example, ensuring that a young user is not exposed to 18+ content requires personalising the content the user sees by their age. Some age verification methods also rely on profiling - for example, AI is a key tool to help detect users under 18 and ensure they receive appropriate privacy and safety protections that relies on profiling.

We recommend that the DPC considers applying a similar approach as the Age Appropriate Design Code, in recognition that personalisation may in some cases be key for consumers to receive the core service they signed up for and beneficial to users with appropriate safeguards in place. This approach is consistent with the GDPR and other guidance in the Fundamentals; namely, that risks to children should be minimized, without leading to "*a deterioration in the overall user experience and the availability of the central features, for which children primarily access the service*."[18] A blanket restriction on profiling would also result in a lower-quality and less age-appropriate experience for younger users. In order to enable services to meet the stated objective of continuing to provide rich, age-appropriate and safe user experience to young people, we urge the DPC to adopt a risk-based approach that focuses on preventing potentially negative outcomes while continuing to enable positive uses.

It is equally important to note that profiling can be a valuable tool for ensuring young people receive age-appropriate experiences online and for ensuring that the policies we have in place are enforced effectively. We appreciate that the Fundamentals acknowledge the potential use of profiling measures for protecting children's welfare. However, we would encourage the DPC to take an even broader view of the benefits offered by data-driven technologies in support of a holistic approach of providing rich, age-appropriate and safe experiences for young people.

[18] Fundamentals, page 42 (emphasis added).