

IAB Ireland contribution to the DPC Consultation on the Fundamentals for a Child-Oriented Approach to Data Processing

(Response to the public consultation closing on 31 March 2021)

Introduction

IAB Ireland welcomes the DPC's "Fundamentals for a Child-Oriented Approach to Data Processing" (the "Fundamentals") and the opportunity to input into the current consultation on it. As an industry association that brings together a large number of Irish publishers as well as other stakeholders from the digital advertising ecosystem, IAB Ireland has a considerable investment in the DPC being seen to show leadership on issues that citizens care about, particularly in the area of digital media and advertising. IAB Ireland supports an approach to privacy and data protection that will provide strong consumer protections and contribute to the sustainability of advertising as an available revenue stream for news media and other valuable online content and services.

Specific "Fundamentals" that seem relevant and helpful for IAB Ireland's members

We find the following specific Fundamentals to be of particular relevance as our members attempt to comply with EU privacy and data protection law.

- Fundamental No. 2 – Clear-cut consent. The Fundamentals helpfully recall the conditions for valid consent laid down in the GDPR, and the applicability of these conditions for children as well as other data subjects.
- Fundamentals Nos. 5 and 6 – Information in every instance, Child-oriented transparency. The Fundamentals provide helpful advice for data controllers seeking to ensure that their services enable the taking of informed decisions by all users, including children.

Concern in relation to the scope of the prohibition on profiling children

Our key concern with the document in its current state is to do with Fundamental No. 12. It seems at least possible that the virtual prohibition on the processing of children’s personal data for advertising purposes may have the unintended consequence of leading to the elimination of the processing of personal data for advertising for *all* users on sites that fall within scope of the guidance. This is because absent the ability to ensure that the services are *not* being accessed by children, data controllers will be reluctant to risk the high fines imposed by the GDPR for breaches, and will implement the “floor of protection” approach. It is not clear that the DPC has anticipated the sweeping potential impact of this provision, applying as it does to the processing of personal data beyond profiling.

Section 6.2.3 states that organisations “should not profile children, engage in automated decision making concerning children, *or otherwise use their personal data* [emphasis added], for advertising/ marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so”. The same paragraph goes on to say that for the avoidance of doubt, “the DPC does not consider that it is in the best interests of children to show them advertisements or auto suggestions for other games/ services/ products/ videos/ etc. which they might be interested in where such advertisements or suggestions are based on profiling”. The wording appears to leave open the possibility that the processing of children’s personal data for advertising-related purposes other than profiling (e.g., frequency-capping) may meet the “best interests” tests, though this is not explicit. Importantly, the “best interests of the child” standard is subjective and provides no legal certainty for data controllers.

Furthermore, we believe the Fundamentals take insufficient account of the scope for content personalisation to both enhance the user experience for children and safeguard their interests. Content suggested as a result of personalisation may be more suitable to a child's age and interests than if he or she had to rely on proactive searching or have random content suggested. We do not seek to defend the profiling of children *per se* (especially not of young children), or even content personalisation without limitation, since arguably children prior to the age of consent may not be able to critically assess the implications of such personalisation (including potential harms) to themselves. But a blanket prohibition seems to ignore the potential for such personalisation to positively impact children's online experience.

Moreover, the clear prohibition on profiling children on the online services concerned, and the lack of clarity with respect to the processing of their personal data for *non-profiling* purposes, combined with the difficulty of achieving full certainty in age verification, may in practice mean that not only profiling for advertising and content personalisation, but the processing of personal data for *any* advertising-related reasons, is rendered legally risky. It seems unlikely that this was the DPC's intention, but it would be important for the point to be elucidated, e.g. for spam detection, fraud prevention, or frequency capping. With respect specifically to age verification, we would respectfully encourage the DPC to emphasise that age verification should be viewed as one tool amongst a suite of other tools, such as data protection by design and default measures, that work dynamically to ensure age-appropriate online experiences. We stand ready to work with the DPC and other industry partners to develop effective and scalable age verification measures.

We also note that the Fundamentals expressly refer to contextual advertising, outlining that it is out of the scope of data protection law because it does not rely on personal data. However, it would be important for the Fundamentals to clarify that even contextual advertising that implies some processing of personal data is out of the scope of Fundamental 12. Contextual advertising does not imply profiling the individual, but relies on contextual signals such as coarse location (e.g., city) and the site or app the individual is visiting.

Conclusion:

As noted above, we share the DPC's conviction that the effective protection of children online is primordial and a *sine qua non* for the sustainability of the internet and Europe's digital economy. We appreciate the degree to which the Fundamentals align to, and reference, key principles in the GDPR, including the importance of a risk-based approach, accountability of data controllers, and transparency and control for users underpinned by a strong baseline of security conferred by privacy by design and default. We hope to work with the DPC over the coming weeks, as the Fundamentals are finalised, to limit the scope for the unintended consequences cited above.

Dublin, 30 March 2021