



Technology Ireland submission to Data Protection Commission on Fundamentals for a Child-Oriented Approach to Data Processing.

About Technology Ireland:

Technology Ireland is an Association within Ibec, which represents the ICT, Digital and Software Technology Sector. The Association is a pro-active membership organisation with over 200-member companies located throughout Ireland. We advocate on behalf of Ireland's indigenous and foreign direct investment (FDI) technology companies to Government and policy makers.

Summary of Technology Ireland Position:

Technology Ireland is very grateful to the Data Protection Commission for the opportunity to comment on the draft Fundamentals for a Child-Oriented Approach to Data Processing. Technology Ireland acknowledges that data protection law is about everyone's fundamental right to the protection of their personal data including children, and that the protection of children's rights is an area where all organisations, parents/guardians and policymakers must pay particular attention. When personal data is shared with an organisation, the organisation has a duty to comply with laws and regulations governing how that data is handled. We acknowledge too, that children enjoy all the same rights as adults over their personal data – data about them is still their personal data and does not belong to anyone else, such as a parent or guardian.

From the outset Technology Ireland would like to endorse the Commissioner's statement in her foreword that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data.

We are keenly aware of the work that has gone into preparing this draft within a very challenging timeframe. We also recognise the major challenges involved in bringing forward proposals that advance the goals of online safety and protecting children's data in a manner that is practical, technically feasible and consistent with current GDPR regulations.

With regard to the DPC's proposed ban on profiling of children's data for profiling purposes, Technology Ireland believes that profiling is not in itself always contrary to the best interests of children. While the current draft of the Fundamentals does acknowledge this, the use of the term "prohibition" implies an almost statutory obligation. We believe that the same objectives could be met if the aim was clarified to "profiling by exception".

We welcome the DPC's objective of continuing to work with other data protection authorities, such as the ICO, who have developed an Age Appropriate Code, as well as the CNIL and the EDPB, whose work in a similar space is ongoing, to ensure the development of shared, consistent approaches to children's data and to enable interoperability across jurisdictions. This approach will help to deliver a flexible and risk-based approach to children's data protection in the context of their online activities.

Section 32 of the DPA 2018 requires that the DPC encourage the drawing up of codes of conduct to promote best practices by organisations that process the personal data of children and young people. Technology Ireland, through the creation of its Online Safety Taskforce in 2019, is committed to engaging on the development of codes of conduct and supportive of the DPC's plans in this regard. The taskforce is a pro-active, member-led, and inter-company taskforce which strives to develop, communicate, and support the implementation of agreed policy solutions relating to children & online safety matters.

Technology Ireland believes that, while some of these issues may be resolved in subsequent drafts of the Fundamentals, long term success in protecting the interests of children can be substantially advanced through multi-stakeholder engagement and codes of conduct.

We believe that codes of conduct are useful as they allow for new operational responses to technological and societal changes, whilst upholding the Fundamentals and protecting the interests of children. Technology Ireland and its members are committed to taking a proactive role in this important area.

Technology Ireland, while generally supportive of the 14 Fundamentals, does have some concerns as to their implementation, particularly, as detailed below, with regard to consistency with GDPR and with guidance issued by other authorities. We would be grateful to the DPC if these could be addressed and, where necessary, clarified in subsequent drafts. Technology Ireland also invites the DPC to continue to develop their practical approach by providing appropriate information on how other elements of the draft Fundamentals can be operationalised, such as age verification without undermining data protection rights as a consequence.

Specifically, we believe that the draft Fundamentals should:

- Have a clearer focus on the GDPR concept of risk-based approach throughout;
- Ensure that all the legal bases under the GDPR remain applicable, keeping in mind the risk associated with processing children's data. While consent is a primary tool, it should not be

the only one considered. The draft Fundamentals does state this, but it could be made more explicit and reinforced;

- Acknowledge children’s fundamental rights and freedoms, including but not limited to their autonomy and avoid treating older children as lacking capacity;
- Enable organisations to adapt their online services to different children audiences;
- Allow that there are beneficial uses of data for children, which may sometimes involve profiling;
- Acknowledge that when profiling is used, the best interests of children can still be protected by assessing the exact purpose of the processing. This should be considered as part of a wider context, taking in the role that profiling plays in the provided service, together with the safeguards in place to address any likely and serious harm.
- Provide a clear schedule for compliance with the finalised Fundamentals, allowing adequate time for the practicalities of implementing and fine tuning new operational methods.

The main areas of concern are outlined below and broken down according to chapter:

Chapter 2: The landscape of children’s rights

(2.1 Best interests of the child; 2.4 Legal bases for processing children’s data)

- Fundamental 3 - “Zero Interference” states 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 interest of the child.* This suggested threshold does not appear to align with the concept of legitimate interests, which acknowledges the possibility of balancing the rights of children, although setting a higher threshold for doing so. We would suggest that the DPC ensures that draft Fundamentals does not unintentionally restrict the application of a legal basis expressly provided by law.
- There is no clarification in the text as to what exactly is meant by “Interference”. The examples provided in the draft Fundamentals of scenarios where the legitimate interests basis is unlikely to be unavailable primarily relate to profiling and targeted / behavioural advertising but given that the draft Fundamentals prima facie prohibits such processing in any case, these are perhaps not the most helpful examples. As drafted, the commentary in the draft Fundamentals on this point could be taken to mean there should be zero interference, whether positive or negative, which does not appear to reflect the DPC’s true aim.
- We note that the DPC refers at times in the draft Fundamentals to the “vital interests of the data subject” and in other places to the “best interests of the child”. As these terms may be interpreted differently, it may be useful for the DPC to refer to one of these terms throughout the draft Fundamentals to prevent any inference by others that these are different concepts.
- The draft Fundamentals seem to broadly view all commercial services as going against the best interests of the child. Technology Ireland would suggest a more nuanced, risk-based approach that acknowledges the very broad variety of commercial services, including many

that are harmless or indeed beneficial to children. A controller should be able to take this into account during a risk-assessment, while also considering additional factors like the evolving capacity of children. An example could be the advertising of tutor services to children studying for exams. Also, it is not clear on whether this applies only to organisations directly offering commercial services to children (e.g., games that allow children to purchase add-ons, or where the service is funded by advertising). In particular, we recommend the DPC clarify that the “zero-interference” Fundamental does not mean that legitimate interests cannot be a valid legal basis if an appropriate balancing test is carried out, in line with GDPR requirements. Such a test does not require zero interference with the data subject’s fundamental rights and freedoms, but rather an assessment of whether those rights override the legitimate interests pursued in the context at hand. The same test should apply where children’s data is concerned. As a guide for organisations carrying out this balancing, it might be helpful for the DPC to specifically provide guidance on the interplay between the best interests of the child and the exercise of other fundamental rights and freedoms of children, in this case, when conducting a balancing test in the context of a legitimate interests assessment.

- Given the recommended restriction on a controller’s ability to rely upon legitimate interests, coupled with the DPC’s note of caution regarding the appropriateness of relying on contractual necessity (due to the “complexities, nuances and antiquated nature of elements of this area of Irish contract law”), the practical consequence of the draft Fundamentals is likely to be either an increased and inappropriate overreliance on consent (despite the draft expressly stating that consent is not the only legal basis and does not take precedence over others, and despite the potential for this to create consent fatigue for children and the authorised holders of parental responsibility) or the cessation altogether of many processing activities carried out in connection with the provision of a service to children. This may in turn frustrate a controller’s ability to fulfil other Fundamentals, especially Fundamental 10 - “Don’t shut out child users or downgrade their experience.”

Chapter 3: Transparency and children

- The draft Fundamentals largely reflects Technology Ireland’s understanding of good practices around notice and transparency for children. However, it also states that we should “provide explanations to children as to why certain settings are automatically switched to off or denied to them by default.” Compliance with this provision may prompt children to lie about their age (e.g., if an organisation expressly tells a child that they are too young to access certain features). Additionally, this requirement arguably extends beyond a controller’s GDPR obligations.
- The draft Fundamentals advises that “knowing your audience” is fundamental and suggests that this can be done by “conducting user testing, market research, user consultation and artificial intelligence amongst other things”. It appears that the goal here is to provide practical methods by which this principle might be implemented but that it would be up to

the service to decide which specific method they consider most appropriate. Clarification on this point would be useful.

Chapter 4: Exercising children's data protection rights

(4.1 The position of children as rights holders; 4.2 Acting on behalf of a child)

- Technology Ireland appreciates the recognition in the draft Fundamentals of children as data subjects, with the same data protection rights afforded to adults under the GDPR. It would be helpful for the Fundamentals to provide further clarity on whether organisations should apply the GDPR's restrictions to younger users' rights in the same manner they would to adult users. (i.e., as the GDPR expressly states that some rights are not absolute and are subject to limitations; it would be valuable for organisations to understand whether these limitations apply in an identical way to younger users as they do to adults.) When a conflicting request is received (i.e., a parent is seeking to exercise a child's right to access) and a child has (i) not expressed their desire to exercise this right or (ii) they have actively expressed their desire for the parent to not be provided with access to their personal data), should a controller give preference to the data subject themselves?
- How would the DPC suggest data controllers verify requests made by parents / guardians while considering the principle of data minimisation?
- When reviewing a request to exercise a child's data protection rights, should their age be considered before fulfilling it (in light of the DPC's comment "In such situations, the UN Committee's position is that the age and developmental capacity of the child should be taken into account to assess the level of maturity of the child.")? The Convention on the Rights of the Child recognises that individual children have evolving capacities and acquire competencies at different ages and notes that this should be acknowledged in law, policy and practice.

Chapter 5: Age of digital consent and age verification

- Technology Ireland agrees that organisations must seek to strike a balance between providing children a service that mitigates risks specific to them through proportional measures and safeguards, while also ensuring that children's experience of the service is not inferior, which could also compel them to take further steps to lie about their age. However, we would ask that the DPC develops the practical approach it has taken in the draft Fundamentals to include more concrete guidance on how to operationalise age verification and the factors that would be relevant in determining when it is appropriate to age restrict a feature entirely without undermining data protection rights.
- Section 5.6 on Age Verification Systems states that *Where a service provider stipulates that their service is not for the use of children below a certain age, they should take steps to ensure that their age verification mechanisms are effective at preventing children below that age from*

accessing their service. If the organisation considers that it cannot prevent children below its stipulated age threshold from accessing its service, then the organisation should ensure that appropriate standards of data protection measures are in place to safeguard the position of child users, both below and above the organisation's official user age threshold.

As such, the emphasis appears to be on preventing underage users from accessing the service. This would require a large degree of upfront and potentially excessive collection of data and subsequent processing at the account registration stage. This could create a tension with the requirements for proportionality. It could also have the unintended and unwanted effect of dampening the empowering nature of the GDPR and reducing the levels of active exercise of rights.

- Section 5.3 on Age Verification Purposes notes that age verification is not an explicit requirement for compliance with Article 8 of the GDPR. However, it then goes on to state that it is often the “*practical implication of Article 8 in most cases*”. In order to avoid unintentionally introducing any ambiguity as to what compliance with Article 8 of the GDPR requires, Technology Ireland recommends that it would be beneficial if the draft Fundamentals not only makes it clear that age verification is not required to comply with Article 8 but also includes specific examples of circumstances when it would not be necessary. e.g., where an organisation relies on parental consent for all of its users of its services and therefore does not need to verify the age of any of its users.
- The role of parents and guardians is critical also. Where parents or guardians facilitate or tolerate children having access to services not designed for their age band that can pose risks for children and possibly also privacy concerns for other legitimate users of the service. The Fundamentals should encourage any actions which help to educate or support parents and guardians in protecting children and making them aware of the risks inherent in facilitating children to circumvent appropriate age restrictions.
- It would also be helpful if the draft Fundamentals suggested proportionate mechanisms such as the use of a neutral age gate and then working proactively to detect and remove underage users, who have circumvented the measures deployed at the account registration stage.
- While we note the DPC's view that industry should innovate to create age verification mechanisms which meet the standards required in the draft Fundamentals, the DPC should explicitly acknowledge that those mechanisms may not yet exist and that currently no age verification mechanism is entirely infallible or free of risk.
- The DPC acknowledges that it has no competence to tell organisations which audience to target in their products and services but goes on to say that limiting access to a service to adults does not prevent one from having to comply with the guidance because there is a risk that a child would circumvent verification controls. We would welcome further clarity from the DPC on this point and the recognition of the risk-based approach as well as the limitations of current technology, which at the moment is not able to provide verification with full certainty. Similarly, it may be difficult to ensure that appropriate consent is collected where required in accordance with the requirements of the draft Fundamentals, where a floor of protection is implemented instead of tailored age verification. For, example where consent is

collected by a business for a certain processing activity, it may not be clear to the controller that they are engaging with a child and so the requirements for consent may be unclear.

- Technology Ireland believes that age verification should be viewed not as a single tactic, but rather as a collection of ongoing efforts that work dynamically to provide effective solutions. Effectively verifying age should not focus on a single-step process, but rather a holistic approach that works dynamically to ensure users receive the right experiences according to their age. Closer industry collaboration is also critical to developing effective and scalable measures to ensure young people receive age-appropriate experiences across the online ecosystem. We believe that the draft Fundamentals are consistent with such a response but a more explicit emphasis on the importance of collaboration among industry and policymakers, involving children and parents would be helpful.
- It would also be helpful that the DPC provides guidance on the “reasonable means” likely to be used by companies, which do not consider asking for IDs –as such request for documentation would neither be necessary nor proportionate for most online services. It would be of particular interest to know whether practices such as inference of metadata, data related to users’ activity online and content data are acceptable, if backed by a rigorous and comprehensive use of a DPIA. Separately but concurrently, are practices such as “buttons” available online to empower other users to flag users that are probably under-age acceptable?
- Finally, end users should have an input on what constitutes their reasonable expectations, which may vary from one service to another. We would recommend a practical approach in which data controllers would be entitled to carry out targeted surveys with their specific users, should they be willing to know more. Such surveys could either usefully target categories of users based on their age, children or legal guardian. Therefore, we would be keen on knowing more about the position of the DPC regarding such “targeted surveys” and the way the DPC considers data controllers should take those into account –notably when carrying out a DPIA.

Chapter 6: Direct marketing, profiling and advertising

- As outlined above Technology Ireland believes that profiling is not in itself always contrary to the best interests of children. While the current draft of the Fundamentals does acknowledge this, the use of the term “prohibition” implies an almost statutory obligation. We believe that the same objectives could be met if the aim was clarified to “profiling by exception”.
- In Section 6.2.3 of the draft Fundamentals, the DPC offers its own interpretation of processing which it considers not to be in the best interests of the child, such as advertising to children or offering automated suggestions for content based on profiling. While Technology Ireland fully agrees that the rights and welfare of children must be recognised and protected within data protection law, this must be rooted in the principles of data protection law contained in the GDPR.
- It would be helpful if the draft Fundamentals acknowledged that where profiling is used, the best interests of children can still be protected by assessing the exact purpose of the

processing. This should be considered as part of a wider context, taking in the role the profiling plays in the provided service, together with the safeguards in place to address any likely and serious harms. Technology Ireland's view is that profiling is not in itself always contrary to the best interests of children. Some practical guidance on how to build safeguards around profiling for specific purposes would also be useful. We acknowledge the DPC's confirmation in the draft Fundamentals that contextual advertising falls outside of the remit of data protection law as it does not rely on personal data. However, it would be helpful if it could be further clarified that even contextual advertising that does rely on some element of personal data is also not captured by the draft Fundamentals, in particular with respect to any ban on profiling (Fundamental 12). Contextual advertising works by using contextual information, such as the website or app that an individual has viewed, a recent search query they have made or the city they are located in, to serve more appropriate ads to that individual. It does not entail creating a user profile or using personal data associated with their account for targeting them with advertisements. Furthermore, as is the case for any ad serving operation, a certain element of ad measurement, spam and fraud detection and frequency capping is required, and we would suggest that the draft Fundamentals makes it clear that such processing activities do not amount to profiling.

- Additionally, it may be helpful for the DPC to review the "Profiling Standard" of the ICO's Age Appropriate Design Code, which requires profiling be switched off by default. An outright prohibition on profiling as suggested in Fundamental 12 may create a situation in which a service is markedly different depending on whether it is offered to users in the UK or in Ireland.
- It is worth noting also that Audiovisual Media Services Directive 2018 (AVMSD), which is due to be transposed into Irish law, does not prohibit profiling of children.
- The "Children's Communication Code" issued by the Broadcasting Authority of Ireland (BAI) in 2013, does not prohibit targeted advertising to children, but lists rules and safeguards to protect children.

Chapter 7: Tools to ensure a high level of data protection for children

- Fundamental 13 – "Do a DPIA" is a useful suggestion but would benefit from more explicit practical guidance including a template from the DPC.

Implementation Period

It would be useful also if the DPC could provide a timeline for implementation of the guidelines once they are finalised. We hope that our comments and observations in this submission are useful to

ensuring that rights of children regarding their data are upheld and protected in a manner that is practical and feasible and consistent with existing regulations.

Code of Conduct to support the Fundamentals

As stated at the start of the submission, Technology Ireland supports the DPC intention under section 32 of the DPA 2018. Through the establishment of its Online Safety Taskforce, members are committed to engaging in multi stakeholder engagement and the development of codes of conduct.

Conclusion

Technology Ireland is strongly supportive of the overall objectives of the draft Fundamentals for a Child-Oriented Approach to Data Processing. We recognise that this consultation is only part of an ongoing dialogue with stakeholders. Technology Ireland and its members remain committed to supporting and valuing the work of the Data Protection Commission and look forward to participating in future discussions.