Submitted on: 26 March 2021

# Centre for Information Policy Leadership Comments on the Data Protection Commissioner's Draft Guidance entitled Children Front and Centre – Fundamentals for a Child-Oriented Approach to Data Processing

On 20 December 2020, the Data Protection Commissioner for Ireland (DPC) issued her draft guidance on the safeguarding of the personal data of children when providing online services, namely "Children Front and Centre—Fundamentals for a Child-Oriented Approach to Data Processing" (Draft Guidance).[1] The DPC invited public comments on the document by 31 March 2021.

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit its comments and recommendations below as input to the DPC final guidance.

**Summary of CIPL Recommendations:**

- The DPC should work with other data protection authorities, especially in Europe, to ensure the development of shared, consistent interpretation and approaches to children's data processing and to enable interoperability across jurisdictions;
- The DPC should generally develop and apply a flexible, outcome-driven and risk-based approach to children's data protection in the context of their online activities;
- Specifically, the Draft Guidelines should:
    - Clarify the scope of organizations to which the Draft Guidance apply;
    - Have a clearer focus on, and leverage, the GDPR concept of risk-based approach;
    - Clarify issues regarding the requirement to verify the age of users;
    - Not be prescriptive;
    - Clearly link the list of design and default measures to the substance of the Draft Guidance;
    - Acknowledge children's other fundamental rights and freedoms including, but not limited to, their autonomy;
    - Take a risk-based approach to profiling; acknowledge that when profiling is used, the best interest of the child should be assessed paying particular attention to the purpose of the processing, the role that profiling plays in the provided service and the safeguards put in place to address likely and serious harms. In addition, the Guidelines should recognise that there are also beneficial uses of children's data, including through the use of profiling;

[1] Children Front and Centre—Fundamentals for a Child-Oriented Approach to Data Processing; DPC draft version for public consultation available at <https://www.dataprotection.ie/sites/default/files/uploads/2020-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_Draft%20Version%20for%20Consultation_EN.pdf>.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

- Enable organisations to adapt their online services to different children audiences and provide examples of how to do so; and
- Provide that the obligation not to "downgrade" services should only apply to services intended for children.

## 1. RELATION WITH OTHER REGULATORY GUIDANCE ON CHILDREN'S DATA PROTECTION

The Draft Guidance adds to a growing body of work carried out by regulators, including the UK Information Commissioner (ICO) in their Code of Practice for Age Appropriate Design for Online Services (ICO Age Appropriate Code), which has been approved by the UK Parliament.[3] CIPL notes that work on this issue is also being conducted by the French data protection authority, the *Commission Nationale de l'Informatique et des Libertes* (CNIL)[4] and by the European Data Protection Board (EDPB).[5]

**CIPL encourages the development of shared, consistent approaches to children's data to enable interoperability across different jurisdictions (especially in Europe).** This includes both the development of a common interpretation of GDPR requirements as they relate to processing of children's data, as well as a common broader approach to protection of children in data processing situations. This should incorporate a robust set of standard principles while, at the same time, offering flexibility for controllers to adapt pragmatic and innovative approaches and respond to a variety of children's needs and developmental stages.

### 1.1 The Draft Guidance and the ICO Age Appropriate Code

Overall, CIPL notes that the fundamental approaches of both the Draft Guidance and the ICO Age Appropriate Code have much in common and are largely consistent, including a focus on the centrality of the interests of the child as a guiding principle and the adoption of a risk-based approach in some areas. However, they do have some fundamental differences that should be considered by the DPC. CIPL considers it important for service providers to be provided with consistent guidance by regulators in the area of protection of children's data and welcomes those elements of consistency.

The key differences between the Draft Guidance and the ICO Age Appropriate Code, as well as the legal regimes of these two countries, are as follows:

- **Scope**. CIPL recognises that the scope of the Draft Guidance is not identical to the ICO Age Appropriate Code. However, unlike the ICO Age Appropriate Code, the Draft Guidance:

[3] UK ICO Age appropriate design: a code of practice for online services, 2 September 2020, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>.

[4] In 2020, CNIL undertook a public consultation on the rights of minors in the digital environment (see here <https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique>) and is due to issue guidelines with legal clarifications and practical advice.

[5] The EDPB has included recommendations on children's consent and flagged children as a particular area of concern in the GDPR in their 2020 Guidelines 05/2020 on consent under Regulation 2016/679, available at <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

- Applies to all organisations that process children's data, not just providers of Information Society Services ("ISS"); and
- Has a broader scope compared to the ICO Age Appropriate Code that focuses on aspects of design, in particular, while the Draft Guidance includes issues such as the appropriate approach to migration of data and services when children reach adulthood, how to address security standards, handling data breaches, and the use of biometrics. We would suggest that the DPC considers whether there is a way to reconcile this approach with the approach adopted by the ICO, as discussed further at (2) below.

- **Age of consent**. CIPL also recognises that when the legal basis for the relevant processing activity in relation to information society services is consent, the age of consent is 16 years under the Irish data protection legislation, whereas it is 13 under the UK regime. This difference is reflected in some of the Draft Guidance to the extent it involves the role of parents and guardians.
- **Profiling**. The ICO Age Appropriate Code does not propose an outright prohibition on profiling of children, but instead requires safeguards and mitigation of harmful effects for the child, if any. However, the Draft Guidance takes a blanket approach that profiling and best interests of the child cannot coexist, which CIPL does not accept as necessarily being the case.
- **Default privacy settings**. The Draft Guidance states, "where a child switches off a default privacy setting, at the end of a session this should automatically switch back to the default settings." The ICO Age Appropriate Code only requires this in relation to geolocation.

## 2. SPECIFIC COMMENTS TO THE DRAFT GUIDANCE

CIPL welcomes the DPC's statement in the Foreword to the Draft Guidance that there are not necessarily clear-cut answers about what is "right" and "wrong" in online activities in every case. The DPC cites the debate about the age of consent and differing views. **CIPL encourages the DPC to develop and apply a flexible, outcome-driven and risk-based approach to children's data protection in the context of their online activities**. CIPL further supports the DPC's practical outlook on the protection of children's data, for example, by including a floor of protection model in its Draft Guidance. CIPL invites the DPC to continue to develop this practical approach by providing appropriate information on how other elements of the Draft Guidance can be operationalised, such as age verification.

CIPL also welcomes that the DPC solicits responses from other EEA regulators, recognising that the standards set for global internet service providers established in Ireland will affect all child data subjects throughout the EEA.

CIPL particularly welcomes the commitment in the guidance to the importance of safeguarding children, and the stated position of the DPC that child protection/welfare measures should always take precedence over data protection considerations affecting an individual. As the DPC notes, "The GDPR, and data protection in general, should not be used as an excuse, blocker or obstacle to sharing information where doing so is necessary to protect the vital interests of a child or children."

Both domestic and multinational organisations often face instances where data protection obligations conflict with other obligations in other regulations. We support this explicit statement in the Draft Guidance as a proper and appropriate balance.

### 2.1 Structure of the Draft Guidance—the Fundamentals

The structure of the Draft Guidance sets out 14 "Fundamentals" (Fundamentals) as the guiding principles for organisations to follow when processing the personal data of children. These Fundamentals are presented as "sound bites" to be brief and memorable and then further explained by the DPC. For ease of reference, CIPL has listed and summarised the Fundamentals in the table below:

| Fundamentals of the Draft Guidance | Explanation |
|---|---|
| **1. Floor of protection** | Controllers should either take a risk-based approach to verifying ages so they can offer appropriate protection to children or build their services so that they apply all the fundamentals to all users. |
| **2. Clear cut consent** | Any consent must meet the full GDPR consent standards. |
| **3. Zero interference** | The pursuit of legitimate interests should not negatively impact the best interests of the child in any way. |
| **4. Know your audience** | Organisations should take steps to identify users and implement child protection measures in services directed at or likely to be used by children. |
| **5. Information in every instance** | Transparency is always required directly to the child, even if processing takes place in reliance on parental consent. |
| **6. Child-oriented transparency** | All notices must be suitable for children. |
| **7. Let children have their say** | Organisations must respect the rights and capacity of children. |
| **8. Consent does not change childhood** | The consent of an adult parent or guardian or of the child does not mean children can be treated as adults. |
| **9. Your platform—your responsibility** | Companies that make money from online services pose particular risks. Where such companies use age verification and/or parental consent, they must "go the extra mile" to make sure those mechanisms are effective. |
| **10. Don't shut out child users or downgrade their experience** | Where services are intended for children or likely to be accessed by them, providers cannot bypass obligations by shutting out children or depriving them of user experience. |
| **11. Minimum user ages are not an excuse** | Theoretical thresholds for user age do not displace obligations to comply. |
| **12. Prohibition on profiling** | Controllers should not profile or use automated decision-making to deliver marketing/advertising to children due to their vulnerability, unless they can show it is in the best interests of the child. |

| Fundamentals of the Draft Guidance | Explanation |
|---|---|
| **13. Do a Data Protection Impact Assessment (DPIA)** | DPIAs should be specific in relation to child users. |
| **14. Bake it in** | Controllers should have consistently high standards for processing children's personal data by design and default. |

### 2.2 General issues identified in the Draft Guidance and CIPL recommendations

CIPL has identified some key practical and strategic issues with the Draft Guidance, including with the Fundamentals outlined above. We address those issues below with recommendations to the DPC that we believe will help strengthen the Draft Guidance.

#### *2.2.1 The Draft Guidance should clarify the scope of organizations to which the guidelines apply*

**The Draft Guidance should avoid capturing all online businesses, just in case any of their users are minors.** In addition to applying to services that are "directed at or intended for children," the Draft Guidance states that it also applies to services that are "likely to be accessed by a child." This can potentially be any service offered online. Instead of referring to "access by a child," the scope of the guidance should be narrowed down to a service that is "reasonably likely to be largely used by a child." This would exclude incidental, unintentional or limited access to a service by a child, when the service is otherwise not specifically tailored to children as part of the organization's core business. For the same reason, the Draft Guidance should limit the scope of the suggested "floor protection" (i.e., "treat all your users as children, unless you verify their age") to obvious situations where a service is largely used or intended to be used by children, as opposed to any other online service where the use of the service by a child is likely to be incidental or involve an adult's details (where a minor makes purchases in an online store using an adult's credit card, for example).

#### *2.2.2 The Draft Guidance should have a clearer focus on and leverage the GDPR concept of a risk-based approach*

Although the Draft Guidance provides for a "floor" of protection, generally, the Draft Guidance does not fully reflect the concept of a risk-based approach that is embedded in the GDPR.[6] There are a number of instances where the DPC could have a clearer focus on the concept of a risk-based approach in its Draft Guidance:

- **The DPC could generally recognise that not all processing of personal data relating to children raises the same level of risk.** Article 5 of the GDPR includes accountability and fairness as overarching data protection principles. In assessing the level of risk and the obligation to be fair in processing data, organisations should take into account a matrix of issues to reach balanced judgments. In the context of children's data processing, these include, for instance (i) the age and capacity of the child (e.g., recognising that a 17 year old

[6] See CIPL paper on "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR," 21 December 2016, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>.

has very different capacity and needs than a seven year old), (ii) the nature of the service offered and processing of children's data in that context, and (iii) the appropriate balance between various aspects of children's rights and welfare, including their privacy, access to information, and the possibility of offering richer and more relevant user experiences where appropriate;

- **The DPC should apply a case-by-case, risk-based approach to the concept of commercial online services, rather than a broad-brush approach that may not comport with the reality of risks posed to children**. The Draft Guidance assumes that there is an inevitable conflict between the commercial interest and the best interest of a child. However, this is not necessarily the case. Children do engage in some commercial activity increasing as they mature. It is important that children learn how to engage in commercial activity in an appropriate way. The Draft Guidance (i) does not explain why or which commercial/profitable services pose significant harms or risks to children, such that a blanket approach is justified, and (ii) does not clarify 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. CIPL would suggest that, in practice, this concept of commercial service may not be the most reliable proxy for the level of risk. For example, sites that encourage children to record weight and diet and that may support eating disorders or encourage the posting of inappropriate photographs will likely be high-risk, but not necessarily commercial. Conversely, a child-appropriate game that allows the purchase of add-ons may be commercial, but low-risk; and
- **The DPC could acknowledge that while the protections applied to children may need to be different to those applied to adult users, they may not necessarily be uniformly "higher" protections**. Controllers should apply levels of protection appropriate to the risks of their processing activities as a matter of general compliance and accountability under the GDPR. According to Recital 38 of the GDPR, children merit "specific" protection. CIPL notes that there are several references in Section 1.3 of the Draft Guidance to service providers offering a "higher" level of protection for children's data, not just "specific" protection. For example, the transparency requirement of the GDPR may be delivered in a different and specific way to a child, through use of simpler language, visuals, storytelling, videos, games and other user-design driven tools. This does not necessarily result in a *higher* level of protection, but one that is more specifically tailored to children.

#### *2.2.3 The Draft Guidance should take a practical and proportional approach to age verification*

**The Draft Guidance should clarify when organizations are required to verify the age of their users, especially if the scope of the Guidelines remains broad.** Estimation of age brackets may be preferable to collection of specific ages (e.g., month and year of birth). The age verification topic would benefit from frank and constructive exchanges in a workshop between impacted controllers and the DPC to flag genuine technical challenges and discuss potential solutions.

In the meantime, the DPC should: (i) limit the scope of the age verification requirement to services that are specifically targeted at children, or have a high likelihood of being visited by children because of the nature of the service or goods (as opposed to any online services, eCommerce platforms and retailers which may have an occasional younger customer); (ii) clarify whether age verification is

required mainly for registered users as opposed to mere browsing users with whom an organization does not have a direct relationship; and (iii) clarify whether age verification can be achieved on websites and apps through the user expressly agreeing to relevant age terms and conditions (for example, "by clicking I agree, you confirm that you are not under the age of 13"…).

#### *2.2.4 The Draft Guidance should not be prescriptive*

The Draft Guidance should be outcome-driven and should avoid mandating prescriptive or granular requirements with respect to design and how to provide transparent information. These would risk quickly becoming obsolete, as well as hindering development of more innovative solutions from emerging technology. The prescriptive approach fails to account for developments in the digital literacy of both parents and children in the context of how their specific services are built, targeted, what risks they may pose, as well as the mitigations that may already have been built in, and the ability of organisations to determine what solutions work best for them and their consumers. Biometrics, for example, can be a useful identifier or a security mechanism or may even be necessary to provide the service. Further, on-device processing may not be technically possible for all processing operations or services.

In addition, the Draft Guidance encourages the development of sectoral codes of conduct for children's data under the General Data Protection Regulation (GDPR). While CIPL agrees that such codes of conduct can potentially be useful vehicles to adapt common principles to the specific questions faced by industries, we caution against the imposition of overly granular rules in such sectoral Codes of Conduct. Those sectoral codes of conduct could bring inconsistency in the approach to children's data processing between sectors and could potentially create legal uncertainty and confusion for child users as well.

#### *2.2.5 There is an imbalance between the list of design and default measures and the substance of the Draft Guidance*

In practical terms, controllers using the Draft Guidance may turn to the list of design and default measures that the DPC recommends, as it seems to offer help with practical implementation. However, this list seems very prescriptive even though the Guidance states that these are "examples" of design and default measures that the DPC considers appropriate in the context of children. It is also quite difficult to relate some of these to the Fundamentals or to the rest of the content of the Draft Guidance. Some of the measures are not mentioned at all in the guidance, e.g., restricting data to device-level processing.

CIPL recommends that the DPC review the list of design and default measures to make it clear that they are illustrative examples and link the examples to the substantive guidance in the body of the Guidance rather than adding them as a separate list. We comment on specific design and default measures in more detail below.

#### *2.2.6 The Draft Guidance should acknowledge children's fundamental rights and freedoms including, but not limited to, children's autonomy and take a risk-based approach to profiling aligned with the GDPR*

As the DPC notes, there is currently much discussion at both a global and European level on how to protect children and facilitate their development in the digital environment. Efforts to enhance privacy

for young people require a delicate balance between age-appropriate protection and ensuring children are empowered to develop their confidence, autonomy and resilience online. The protection of their right to privacy, and other rights under the UN Convention on the Rights of the Child, such as their right to association, play, access to information, right of education and freedom of expression are as important as, and should be balanced against, measures aimed at protecting their safety.

The Draft Guidance would benefit from a clearer recognition of the importance of service providers respecting the developing autonomy of young people and empowering them to draw the benefits of online services in a safe and responsible way as they grow and mature. The Fundamentals should avoid requirements that have the effect of treating older children as lacking capacity, which may be unrealistic and encourage teens to look for workarounds to the protections in place. In addition, treating children as lacking capacity may be in conflict with their best interests, such as when children are in vulnerable situations or subject to abuse or undue influence where they would benefit from full autonomy over their data. Organisations should be generally required to adopt a risk-based approach with regard to the age and capacity of a child.

#### *2.2.7 The Draft Guidance should acknowledge that when profiling is used, the best interest of the child shall be assessed paying particular attention to the processing purpose, the role this profiling plays in the service provided and the safeguards in place to address harms*

The DPC's current approach to profiling significantly exceeds that of the GDPR. The European Commission has previously confirmed that it is contrary to EU law for a Member State to unilaterally prohibit a category of processing activity which might otherwise be lawful under the GDPR. That profiling of children is not prohibited by the GDPR provided Article 22 and other provisions of the GDPR are complied with and such processing takes into account the special protections afforded to children.[7] Article 22 is of relevance only when processing constitutes "solely automated processing" that produces "legal effects or similarly significant effects". It is unlikely that a processing of personal data for personalised content or advertising purposes will have any "legal effects," or would affect users in a way that is "similarly significant" to legal effect.

The DPC should adopt a balanced approach and acknowledge that profiling, including the delivery of advertising to children, is not, per se, contrary to the best interests of the child. A broad statement that profiling for advertising/marketing purposes will never be in the best interest of the child is not practical guidance, but rather takes an absolute position that conflicts with other risk-based balancing exercises that the DPC encourages controllers to undertake. The DPC also provides little guidance on how to build safeguards around profiling for specific purposes.

For instance, profiling for advertising purposes should be assessed jointly with: (i) the nature of service that is provided (i.e., whether the profiling or personalisation is required as part of a core service or otherwise as part of an ancillary activity), and (ii) the safeguards that organisations have implemented to avoid or mitigate specific harms to all users, or users of the age bracket for which the service is

[7] See the rulings of the Court of Justice in Cases C-468/10 and C-469/10 which concluded that a Member State could not impose additional conditions that would have the effect of amending the scope of Article 7 under Directive 95/46/EC, and Parliamentary Question response Dáil Éireann Debate, Tuesday, 24 July 2018 at https://www.oireachtas.ie/en/debates/question/2018-07-24/628/

designed. For instance, these safeguards could restrict the types of goods or services advertised to children or the extent of advertising, and give notice and choices to children.

Additionally, the Draft Guidance does not address profiling for any non-advertising purpose, such as integrity and safety, which could be particularly relevant to preventing children's access to harmful content. Content that is more appropriate can be recommended when a profile of the child, including their age, is available. Personalisation would also improve a child user's experience. For example, personalisation allows organisations to offer children a focused, interesting and relevant website, ensuring a better experience for the child. It also makes the service more easily navigable, potentially reducing screen time.

We understand that the aim of Fundamental 9 is to avoid providing a downgraded service to children so that children are not inclined to seek out less trustworthy services with fewer protections. However, CIPL proposes that an outright prohibition on profiling is more likely to lead to a downgraded experience, causing this precise behaviour. In addition, a wholesale prohibition on profiling may disincentivise the creation of content for children, affecting the quality and diversity of information and services available to children.

#### *2.2.8 The DPC should acknowledge that there are beneficial uses of data for children, including profiling*

The Draft Guidance should recognise more fully the cases where specific uses of data for services such as geolocation or personalisation may be beneficial for children. As discussed above, personalisation, in particular, may enable the delivery of enhanced or enriched experiences to children, such as recommended reading lists based on the age of the child, and interests shown in previous searches or purchases. This should be reflected more clearly, in particular with respect to the guidance on "zero interference." As drafted, the Draft Guidance could be interpreted to require zero interference, whether positive or negative, which does not appear to reflect the DPC's true aim.

CIPL also recommends that the DPC explicitly allow profiling of children's personal data, as long as: i) the level of profiling serves to deliver an age appropriate and safe experience to the child in accordance with the relevant age bracket for which the service is designed, and ii) the organisation implements appropriate safeguards.

#### *2.2.9 The obligation not to "downgrade" services (Fundamental 10) should only apply to services intended for children*

This Fundamental should be revised to apply only to services that are intended for children. The current wording is broader and requires that even where access to a service is actively limited or targeted to adults, organisations must comply with the guidance where there is a risk that a child may circumvent verification controls. The fact that a child has the ability to access a service does not provide sufficient justification to require organisations to change their business offers to implement the guidance.

### 2.3 Issues and recommendations specific to the elements of design in the Draft Guidance

Section 7.3 of the Draft Guidance includes recommended measures for incorporating data protection by design and by default to promote the best interests of child users. CIPL identified below certain

issues with some of these recommended measures and recommends that the DPC take a flexible and risk-based approach to resolve these issues. We also note that these specific recommended measures are not present in the ICO Age Appropriate Code.

- **"Strictest" privacy may not always serve the best interest of the child in any age bracket**. While the ICO advocates for "high privacy" by default, the Draft Guidance appears to take a more extreme position of "strictest privacy." However, "strictest" privacy will not always be necessary, or may be in conflict with the children's best interests guiding principle and make provision of the core service difficult or impossible. This "strictest" position is clearly not advocated by the ICO, which suggests this is only necessary with respect to geolocation, and otherwise states that users should be given the opportunity to change the default permanently. The "strictest" position is in conflict with other statements of the Draft Guidance such as (i) the user choice (discussed in Section 7.3), (ii) blocking children from accessing the more complete "full" service offering, and (iii) the best interests of the child standard itself (i.e., by potentially impinging on children's fundamental rights and freedoms as data subjects).
- **Account migration and retention**. The Draft Guidance includes requirements for adult account migration and retention. It suggests that data associated with a 16 year old's account should not be automatically migrated to a new account or the matured status of the account once the user is over 16, as the user may not want to keep all the data. CIPL's view is that this imposes an arbitrary and artificial divide. While CIPL supports the view that children should be reminded to review and possibly cull material at regular intervals and given the tools to do so easily, it is overly prescriptive to require every child to carry out a review on reaching 16. Users should have the benefit of straightforward and seamless migration rather than it being a major change in the nature of the service/relationship. The Draft Guidance should address the gradual move towards personal autonomy as adolescents mature, rather than face a "cliff edge" change to service once they reach adulthood.
- **Security**. The Draft Guidance suggests that there should potentially be higher security controls for children's data than for adults. This is not discussed in the core of the guidance, but appears in the list of examples relating to data protection by design and by default. "Default settings [for security controls] should ensure high levels of security rather than more relaxed levels that may be available to adults. Higher security settings for child account data may be appropriate including the possibility of isolating or "air gapping" child personal data from adult personal data." In practical terms, this may cause significant difficulties, particularly as parents may be actively involved in or monitoring an account. It is also unclear what higher standard the DPC would be expecting, as security measures should already meet the appropriate standard for all users and not just children. In addition, the Draft Guidance should provide that where organisations have made sufficient parental controls available that ensure the child's activities are adequately transparent to their parents, this will be taken into account by the DPC in assessing the high security standard for children's data.
- **Consistency of service**. The Draft Guidance states "measures put in place to protect children are demonstrably effective and that they are equally effective whether a service is delivered via a website, mobile device gaming console or other channel." CIPL would question whether this is realistic, particularly as there is also the statement that services should not be downgraded as a result of offering safeguards for children. The DPC should recognise the risk-

based approach that organisations need to take and the fact that, in practice, no measure is failsafe. In many cases, the type of platform or channel will have an impact on the types of measures to be implemented and, potentially, their effectiveness. This is not something that organisations are technically able to solve. For example, the screen space that organisations have to serve notices to users is reduced on mobile when compared to a desktop. Similarly, the mechanisms for parental control may be more limited on platforms over which the developer organisation does not have control.

- **Biometrics**. The Draft Guidance states that data controllers should "avoid the collection and processing of children's biometric data." However, as noted earlier, such data may be useful for identification or security, or even be necessary for the provision of the service. Further, many websites and services that are specific to health data for children should be recognised as valid and worthwhile services. CIPL recommends that the DPC apply a risk-based approach to allow these data to be collected and processed as long as there is a good purpose and stringent safeguards are applied in line with the GDPR's requirements for the processing of biometric data.
- **User-specific privacy settings**. The Draft Guidance advises that the settings should be specific to each user on a shared device. The DPC should provide examples of how service providers can enforce this recommendation, as this is not clear.
- **Device-level processing**. The Draft Guidance recommends that the service provider should opt to process the child's personal data on the device rather than in the cloud. However, this may be unrealistic in the context of increasing use of cloud technology in modern business processes. It also appears to assume that cloud services are inherently less secure than other services. However, there are risks in any storage—in the cloud or in-devices. For example, if a phone or other device is lost or stolen, the user may be deprived of total access to their data and the data may be accessible to a third party. Finally, in practice, it is not always possible to process the data solely on the device. For example, simple access to online services, or in many cases even the mechanisms for parental control, necessarily require processing in the cloud.

## 3. CONCLUSION

CIPL is grateful for the opportunity to comment on the Draft Guidance and hopes that the commentary above will be useful to the DPC's team as they work on the final version. If you would like to discuss any of the comments in this paper or require additional information, [redacted]