CIPL's Response to ANPD Consultation on Draft Guidelines on Suppliers of Information Technology Products or Services: Scope and General Obligations under the Digital ECA

Submitted 15 June 2026

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the ANPD's consultation on its Draft Guidelines on Suppliers of Information Technology Products or Services: Scope and General Obligations under the Digital Statute of the Child and Adolescent (Digital ECA) (the Draft Guidelines).[2]

CIPL has long been at the forefront of global thought leadership on children's privacy and safety, with a dedicated workstream launched in 2021 to address the increasingly complex regulatory landscape and the resulting operational challenges for organizations in the space. In 2022, CIPL published a flagship report on the key issues that continue to shape the field: consent, profiling, age assurance, risk assessment, safety, transparency, and the best interests of the child.[3]

Building on that foundation, CIPL has actively participated in consultations across numerous jurisdictions, convened multi-stakeholder roundtables, supported age-appropriate online experiences for children and teens, and fostered workable solutions across jurisdictions. Our significant body of work in this space[4] reflects CIPL's consistent and principled advocacy in favor of:

- a **risk-based and proportionate approach**, under which compliance obligations are calibrated to the nature, severity, and likelihood of harm to children, rather than applied uniformly across all services and contexts;

---

1 **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 80+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

2 National Data Protection Authority (ANPD), Draft Guidelines on Suppliers of Information Technology Products or Services: Scope and General Obligations under the Digital Statute of the Child and Adolescent, Brazil 2026, available at https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-o-guia-orientativo-fornecedores-de-produtos-ou-servicos-de-tecnologia-da-informacao-no-ambito-do-eca-digital.

3 Center for Information Policy Leadership (CIPL), "*Children's Privacy Policy Paper I: International Issues & Compliance Challenges*", October 2022, available at: https://www.informationpolicycentre.com/resources/protecting-childrens-data-privacy-policy-paper-i-international-issues-and-compliance-challenges/.

4 See https://www.informationpolicycentre.com/project/childrens-privacy/.

- application of the **best interests of the child** standard as an overarching interpretive principle that guides the design and operation of digital products and services, while recognizing children's evolving capacities and their right to participate, express themselves, and access beneficial digital experiences; and
- **technologically neutral, outcomes-focused regulation** that preserves flexibility for organizations to implement effective protective measures commensurate with their business models, avoids prescriptive one-size-fits-all requirements, and remains adaptive to the continuous pace of innovation in the digital environment.

CIPL commends the ANPD for embracing these themes in its Draft Guidelines, and we welcome the ANPD's ambition to provide greater predictability and legal certainty for regulated entities through clear definitions and interpretive criteria.

The Draft Guidelines provide much needed clarity for entities who fall within the scope of the Digital ECA, as well as guidance on the meaning and implications of the duties of prevention, protection, information, and safety for such entities.

CIPL recommends that the final Guidelines clarify their guidance-oriented and non-binding nature, particularly where they interpret open-textured statutory concepts that may require contextual, case-by-case assessments and where additional secondary regulation may ultimately be required for the sake of legal certainty. This would further preserve the distinction between guidance and formal rulemaking and support the ANPD's commitment to dialogue and proportional supervision.

Where the Guidelines refer to present or future technologies, CIPL further recommends that the ANPD clarify that compliance expectations should arise in a concrete and proportionate manner once a product or service is made available in the market, rather than during ideation, research, testing, or development phases. Any subsequent interpretive expansion should be accompanied by clear criteria and reasonable adaptation periods, so that innovation is not chilled by uncertainty about future compliance obligations. CIPL supports continued stakeholder engagement as well as innovative regulatory tools such as sandboxes to foster accountable innovation.[5]

CIPL offers the following comments in a spirit of constructive engagement and with the shared objective to deliver meaningful and proportionate protection for children online while supporting their access to beneficial, age-appropriate digital services.

[5] See CIPL Paper "Learning from Practice: Designing Effective Regulatory Sandboxes," October 2025, available at https://www.informationpolicycentre.com/resources/learning-from-practice-designing-effective-regulatory-sandboxes/. See also CIPL Paper "Getting the Best Outcomes: Pathways for Data Protection and Privacy Authorities," October 2024, available at https://www.informationpolicycentre.com/resources/getting-the-best-outcomes-pathways-for-data-protection-and-privacy-authorities/.

I. Likely Access

The Draft Guidelines identify "likely to be accessed" as the central threshold for determining the scope of the Digital ECA's application. The Guidelines further clarify that the threshold is met when the cumulative presence of three requirements is identified:

(i) probability of use and attractiveness,

(ii) ease of access and use, and

(iii) a significant degree of risk to the privacy, safety, or biopsychosocial development of children and adolescents.

CIPL supports the cumulative nature of this test, in particular, the third element, which notes that the risk must be "significant". These elements are an important proportionality safeguard that ensures the Digital ECA applies where minors are meaningfully likely to access a service and where such access may create risks that go beyond ordinary or de minimis risks to privacy, safety, or biopsychosocial development. CIPL therefore recommends that the ANPD clarify that the "significant risk" element must be assessed concretely, taking into account the nature of the service, the nature and likelihood of potential versus actual harms, and the safeguards and mitigation measures implemented by the provider.

As CIPL has noted in response to other consultations,[6] obligations should not arise where access is merely incidental or where access is likely because parents are sharing devices with their children, for example. Nor should "significant" mean simply a large number of children or that children comprise a substantial percentage of users. Rather "significant" should mean more than de minimis. The measure of significance should be related to how children's access may affect their rights, interests, and well-being.

While the Draft Guidelines appear to reflect this view implicitly, we respectfully ask the ANPD to do so explicitly. As drafted, the Guidelines appear to define "significant" as that which goes beyond "any ordinary risk inherent in life in society or in the use of technologies." While CIPL agrees with this language, we encourage the ANPD to make clear that significance should go beyond "ordinary risks" and be expressly tied to children's fundamental rights and interests.

We commend ANPD for highlighting the need to carry out risk assessments and impact reports. While we recognize that an entity's own internal risk assessment is not binding on the ANPD, we encourage the ANPD to view such assessments as a good faith effort towards compliance, and as relevant evidence of a provider's regular mode of operation, risk controls, and ongoing, evolving accountability measures.

Moreover, a formal risk assessment should not be required in all cases. CIPL asks the ANPD to introduce a non-exhaustive list of service categories that would presumptively fall out-of-scope of the law: For example:

---

[6] See, for example, CIPL Response to the Office of the Australian Information Commissioner's Office (OAIC) Consultation on the Children's Online Privacy Code, July 2025, available at https://www.informationpolicycentre.com/resources/cipl-response-to-the-office-of-the-australian-information-commissioners-office-oaic-consultation-on-the-childrens-online-privacy-code/.

- Websites focused on professional, business-to-business (B2B), or technical topics, which are not designed to be attractive to children, and which present no discernible risk to children's biopsychosocial development;
- Banking, healthcare, travel, and hospitality services where children's access inherently requires either financial capacity or the active, documented intervention of a parent or legal guardian;
- Enterprise and corporate internal services not directed at the public; and
- Services whose content is restricted to direct, professional, or technical audiences and for which the combination of subject matter and access conditions makes meaningful use by children highly unlikely.

Evidence of actual access or use by children and adolescents—including data from the platform itself or from independent research—may be relevant to the "likely access" assessment, but it should not be treated as determinative in isolation. Such evidence should be assessed in light of the cumulative statutory criteria, the methodology used to generate the evidence, the Brazilian relevance and accuracy of the data, the nature of the service, and the safeguards implemented by the provider.

That said, any effort to collect evidence of child access must be proportionate and privacy protective. CIPL warns against mandates that would for example require adults to provide ID or verify their ages just so companies can prove that children are not using their services, as this creates disproportionate privacy costs for adults. Instead, we support less intrusive evidence sources, such as proportionate market research or user-based data from similar services, provided that any such evidence used in supervision or enforcement is methodologically sound and subject to an opportunity for the provider to address its relevance and conclusions. General market-level or population-level studies may provide useful context, but should not, by themselves, establish likely access for a particular service or functionality without an assessment of their relevance to the specific service, feature, user base, period, access conditions, and risk at issue.

We further encourage the ANPD to reexamine the legal presumption of likely access for certain categories of services. As drafted, the Guidelines include services that employ "generative artificial intelligence tools" as presumptively accessed by children. Such a reference poses the risk of capturing all products or services that incorporate generative AI functionality. Professional creative tools, coding assistants, and enterprise productivity applications that happen to feature generative AI—but whose purpose, context, and use cases make meaningful access by children unlikely—should not automatically fall within scope absent specific evidence of meeting all three elements of the cumulative likely-access test.

CIPL recognizes that the ANPD may have a protective rationale for treating certain categories of services, including social media, as more likely to be accessed by children and adolescents, particularly where reliable evidence indicates widespread use. However, such category-level evidence should support, rather than replace, a contextual and rebuttable assessment. Services and functionalities within the same category may differ materially in their design, audience, safeguards, access conditions, and risk profile. Accordingly, a provider should be able to rebut the presumption by demonstrating, through appropriate evidence, that one or more of the cumulative statutory elements are absent in the concrete operation of the service.

The Guidelines should also clarify how "content of interest to children and adolescents" should be assessed in services that host, distribute, rank, or personalize user-generated content. In particular, the Guidelines should distinguish among content produced, licensed, selected, or specifically promoted by the provider; content generated by users; content distributed by third-party advertisers; and content ranked, organized, or personalized through automated systems. These categories involve different degrees and types of provider control and should not be given the same weight when assessing likely access. Where automated systems rank or personalize content, the assessment should consider the purpose of the system, the safeguards attached to it, and whether it is used to support age-appropriate, protective, safety, integrity, or relevance objectives.

CIPL further recommends that the final Guidelines distinguish among different forms of personalization, rather than treating personalization as an inherent risk factor. Personalization designed to promote age-appropriate experiences, filter inappropriate content, limit risky interactions, or support safety and integrity objectives is materially different from personalization designed primarily to maximize engagement. In many contexts, protective personalization is an important means of complying with the duties of prevention and protection because it enables providers to deliver experiences appropriate to the user's age, maturity, and risk profile.

The Guidelines should also provide additional criteria for services that combine multiple functionalities or evolve over time. Many digital services do not fit neatly into a single category and may combine messaging, content distribution, social interaction, gaming, marketplace, educational, or productivity features. Ancillary or secondary features should not, by themselves, reclassify an entire service where the service's predominant nature remains unchanged; any reclassification based on evolving use patterns should be supported by objective evidence, prior notice, reasoned analysis, and a reasonable adaptation period.

II. Editorial Control

CIPL agrees with the ANPD that regulatory obligations must be calibrated to the nature, context, and severity of the risk. In this context, CIPL welcomes the Digital ECA's recognition that services with editorial control could benefit from a differentiated compliance framework. However, to ensure that the Guidelines remain risk-based and proportionate, CIPL recommends that the ANPD broaden its interpretation of this category.

As currently drafted, the Guidelines appear to contemplate a relatively narrow model of editorial control, centered on human curation of content before publication, as illustrated by the *Novidade e Saber Play* example.

CIPL believes that platforms providing specifically curated child or teen versions of their service without human intervention—by incorporating safety-by-design defaults and restricted functionality, for example—are functionally performing a high level of curation that reduces risk sufficiently to merit similar differentiated treatment.

The ANPD's recognition of such efforts would align with the principle of proportionality, as it would ensure that responsible platforms are incentivized to invest in safe, enriching environments and not face disproportionate burdens that might lead them to restrict minors' access to beneficial digital participation.

III. Duty of Prevention

CIPL commends the Digital ECA's articulation of the duty of prevention as a proactive, cross-cutting obligation that spans the entire life cycle of a product or service, from design through to ongoing operation. This is fully consistent with CIPL's long-standing advocacy for organizational accountability[7] as the foundation of effective data protection, where entities are required not merely to comply with specific rules but to demonstrate a proven and documented capacity for protection that is embedded in their governance structures, policies, and technical architecture.

CIPL would, however, caution strongly against a rigid or uniform implementation of this duty. The duty of prevention must be operationalized in a manner that is proportionate to the nature, context, and severity of the risks identified in respect of a specific service. A duty of prevention that applies with equal intensity to all in-scope entities—regardless of whether their service is high- or low-risk to children (such as educational tools with restricted functionality and limited data processing)—would place disproportionate burdens on lower-risk services without delivering commensurate gains in child safety. CIPL therefore urges the ANPD to make explicit in the final Guidelines that the duty of prevention exists on a scale, that the measures required to discharge the duty vary according to the risk profile of the service, and that the duty is one of diligent and proportionate means rather than a strict duty to guarantee that no harm will ever occur.

Moreover, CIPL emphasizes that the duty of prevention is best understood as a cornerstone of organizational accountability rather than as a catalogue of prescribed technical measures. The responsibility and discretion for determining how to operationalize the duty into risk-based controls, policies, procedures, tools, effectiveness metrics, escalation processes, and evidence of continuous review lies with the organization itself, commensurate with its business model, the nature of its service, and its internal governance structures. Outcome-driven and technology-neutral guidance from the ANPD, rather than prescriptive implementation requirements, will best support this approach.

CIPL also recommends that the final Guidelines clarify the limits of complementarity between the Digital ECA, the LGPD, and the Consumer Protection Code. General obligations under those regimes should not be incorporated into the Digital ECA in a manner that expands the statutory duties of providers beyond the legal text or creates duplicative and uncertain compliance standards. Interoperability among legal regimes should respect the scope, enforcement logic, accountability mechanisms, and competent authorities associated with each framework.

CIPL further recommends that the Guidelines clarify that protective defaults may appropriately differ across age groups. The most protective setting for a young child will not necessarily be the same as the most appropriate protective setting for an older adolescent. A graduated approach is consistent with the Digital ECA's recognition of autonomy and progressive development and with children's rights to access information, participate, and benefit from age-appropriate digital experiences.

[7] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/topics/organizational-accountability/.

IV. Duty of Protection

CIPL strongly supports the comprehensive, special, and critical protection of children and adolescents in the digital environment, and we welcome the duty of protection as a meaningful and enforceable complement to the duty of prevention in the strict sense. CIPL particularly welcomes the prohibition on restrictions on online marketing of fixed-odds betting, tobacco, alcoholic beverages, and other harmful products.

With respect to the *best interests of the child* standard, CIPL strongly supports the centrality of this principle in the Digital ECA and its prominence in the Draft Guidelines. The principle reflects the standard set by Article 3 of the UN Convention on the Rights of the Child[8] and is consistent with the approach adopted in leading international instruments, including the UK AADC.

Children's best interests, however, are not served exclusively by restricting the processing of their personal information or by limiting their access to digital services. In many cases, they are served equally by enabling meaningful, age-appropriate digital participation. CIPL recommends that the ANPD clarify that the *best interests of the child* encompass access to beneficial digital experiences, and that processing or services designed to support such experiences may be consistent with those interests. Any risk assessment framework should accordingly weigh both the harms and the benefits of the service to children in a balanced and contextual manner.

Consistent with Article 12 of the UNCRC,[9] which guarantees that children have the right to express their views freely in all matters affecting them according to their age and maturity, regulatory frameworks should provide for a graduated approach that takes into account the child's developmental stage, cognitive maturity, and context of use. Older children and adolescents should not be treated as lacking capacity; doing so risks incentivizing teens to seek workarounds to protections designed for their benefit. An approach to the duty of protection that tips too far toward restriction runs the risk of unintentionally excluding children from the very digital experiences that support their development, learning, and social participation. The ANPD should make clear that the duty of protection is to be applied with this balance firmly in mind.

CIPL recommends that the Guidelines expressly recognize the legitimacy of layered moderation and safety architectures supported by automated systems for detection, triage, prioritization, and response. In large-scale digital services, automated systems may be essential to identify and respond to patterns of harassment, grooming, self-harm, child sexual abuse material, bullying, or other risks quickly enough to protect children effectively. Both automated and human-led approaches are legitimate tools in a provider's moderation toolkit, and providers should remain free to determine, and consequently demonstrate, the most effective combination for their specific context and risk profile. Such systems should be accompanied by appropriate safeguards, including human escalation for complex or severe

---

8 United Nations General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series.

9 UN Convention on the Rights of the Child, Article 12. See also Article 5 (evolving capacities of the child) and Article 13 (freedom of expression and access to information), United Nations Office of the High Commissioner for Human Rights, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

cases, reporting channels, appeal mechanisms, bias mitigation, appropriate transparency, user education, and continuous improvement.

V. Duty of Information

CIPL strongly supports the duty to inform as articulated in the Draft Guidelines, and we agree that the obligation to provide clear, accessible, and adequate information about products and services, including their operating and usage conditions, as well as the risks involved and the security measures adopted, must constitute a genuine effort to ensure effective understanding by the target audience (children, adolescents, and their guardians). We agree that this duty is not fulfilled by the provision of lengthy, technical, or difficult-to-understand legal texts.

That said, CIPL urges the ANPD to adopt an outcomes-driven approach to its guidance, focusing on whether the covered entity has taken genuine and effective steps to ensure that users and their guardians actually understand how the service works, what data is collected and why, and what risks its use may entail. Such an approach should expressly accommodate innovative, age-appropriate communication formats—including visuals, storytelling, interactive videos, targeted notices, pop-ups, dedicated pages, just-in-time disclosures, and feature-specific explanations provided at relevant moments in the user flow—tailored to the child's developmental stage and maturity level. Furthermore, it should allow entities flexibility to determine which formats work best for their particular services and user base, while recognizing that transparency obligations must be balanced with the protection of trade secrets, security-sensitive information, and technical details whose disclosure could undermine safety or integrity.

Moreover, CIPL urges the ANPD to recognize contextual allowances where the duty to inform may lie at the institutional level—as in cases where an edtech provider contracts with a school or educational authority that itself manages individual student accounts. To the extent the duty to inform may require certain disclosures necessary for informed consent, for example, the agreement governing deployment and use of the service should be recognized as a valid basis for consent. In school settings, requiring individual parental consent at the point of download or account creation for every child and adolescent is not practical and does not reflect how educational technology is actually deployed. The ANPD might consider the COPPA framework in the United States, which recognizes that schools may consent on behalf of parents for educational tools deployed in the classroom.

VI. Duty of Safety

CIPL supports the duty of safety to ensure the responsible operation of digital products and services, and we welcome the Draft Guidelines' recommendation of reasonable measures proportionate to the characteristics of the service, its functionalities, its scale, and the degree of interference it exercises over content and interactions. Such risk-proportionate framing is precisely the approach CIPL advocates. At the same time, the final Guidelines should clarify that scale or reach should not, by themselves, be treated as sufficient grounds to increase obligations without considering the safeguards already incorporated by default and by design. The assessment should consider both the service's potential impact and the mechanisms it uses to reduce inherent risks. It should also consider safety settings, content controls, reporting tools, age-appropriate defaults, integrity systems, and continuous monitoring of effectiveness.

VII. Conclusion

Overall, CIPL appreciates the ANPD's continued and extensive engagement with stakeholders in the development of the Draft Guidelines. The Draft Guidelines reflect considerable thought and incorporate a number of internationally recognized best practices in the area of children's online protection. CIPL respectfully encourages the ANPD to further strengthen the final Guidelines by clarifying the guidance-oriented nature of the document, preserving the cumulative likely-access test, framing presumptions as rebuttable, providing procedural safeguards for reclassification, and recognizing protective personalization and layered safety systems. Mitigating factors, good-faith compliance efforts, and reasonable adaptation periods when new obligations are introduced should factor in any enforcement considerations, and the guidelines should be reviewed and adapted in regular intervals to account for new developments.

CIPL stands ready to engage further with the ANPD on any of the issues raised in this response, including through bilateral discussion, participation in workshops, or contribution to subsequent consultations on the implementation guidance that will accompany the final Digital ECA framework.