GNI Statement on the Preliminary Orientative Guide on Age Assurance Mechanisms

Introduction

The Global Network Initiative (GNI) welcomes the opportunity to provide feedback regarding Brazil's preliminary Orientative Guide on Age Assurance Mechanisms, published in May 2026 by Brazil's National Data Protection Agency's (ANPD). The Guide provides interpretive guidance translating obligations under Law No. 15,211/2025, the Digital Statute for Children and Adolescents (ECA Digital), and Decree No. 12.880 into operational detail. As such, it introduces consequential choices that expand the practical reach of mandatory age assurance to general-purpose infrastructure and positions biometric methods as a standard rather than exceptional tool.

GNI is the preeminent multistakeholder organization dedicated to advancing freedom of expression and privacy in the information and communications technology (ICT) sector. GNI brings together leading ICT companies, civil society organizations, academics, and investors around a shared framework grounded in the UN Guiding Principles on Business and Human Rights and international human rights law, including the ICCPR. Through this multistakeholder collaboration, GNI works to protect and advance the rights of users worldwide as governments and companies make decisions that affect freedom of expression and privacy online.

GNI has engaged with child safety and age assurance frameworks in other jurisdictions. GNI's consistent position has been that the protection of children and adolescents online is an important aim, but that measures pursuing this legitimate aim must be clearly defined, carefully crafted, and proportionate, in line with international human rights law, in order to ensure the protection of the privacy and freedom of expression of all individuals, including adults. GNI welcomes ANPD's effort to ground implementation in a risk-based, proportionality-driven framework. In particular, GNI deeply appreciates the Guide's emphasis on data minimization, its preference for verifiable credentials, and its prohibition on secondary use and traceability of assurance data.

I) Impact on Adult Users and the Limits of the Proportionality Framework

Age assurance mechanisms, although designed to protect children, are encountered by the entire user base of the digital service, including adults seeking to access lawful content. GNI appreciates that the Guide acknowledges this reality in Section III.1, which notes that adverse effects can reach both minors and adults. GNI encourages ANPD to make this principle central and operational throughout the Guide.

For example, a 2025 breach at Discord's third party vendor, exposed government identity documents submitted by roughly 70,000 users for age verification, after attackers compromised a third-party vendor the platform relied on to process those documents. The incident illustrates that the privacy risks created by an assurance mechanism can, in practice, exceed the risk it was deployed to mitigate.

Beyond this security risk, the reality is that simply asking for identification creates a barrier to access and while such barriers may be easily surmounted by individuals with ready access to required documents and tools, they are likely to be have disproportionate impacts on disadvantaged populations whose socio-economic status, gender-identity, race, language, and/or age may make them less likely to want or be able to take additional steps to access information. ANPD should treat any chilling effect on lawful expression or access, including self-censorship arising from reluctance to submit biometric data or identity documents, as a relevant risk under the proportionality requirement in Section III.1, not solely as a data protection risk addressed under Section III.3. Providers should also be expected to assess and report how a given mechanism affects adult access to lawful content, not only its accuracy for identifying minors.

II) Scope and the Limits of "Likely to Be Accessed"

The Guide, consistent with the ECA Digital, applies to providers of products or services "directed at children and adolescents, or likely to be accessed by this audience." A service therefore does not have to be designed for children to be affected. GNI has raised concerns about scope provisions of this kind before, noting in its comments on Colombia's draft Childhood Protection Law that vague definitions and broad obligations across an unclear range of intermediaries create significant risk for freedom of expression and privacy.

Applied broadly, the "likely to be accessed" standard could impact a wide range of general-purpose digital infrastructure providers, including small and non-profit providers, operating systems, digital encyclopedias, and other services which present minimal risks to children and/or have limited ability to implement age assurance.

For instance, operating systems can often be copied or run without any centrally managed account, which makes it structurally difficult to attach a reliable age signal to a specific user, and developers of several Linux-based systems have stated publicly that age verification is neither technically achievable nor appropriate for open source software. ANPD should clarify how the proportionality and risk-based principles in Section III.1 apply to providers in this position, so that the practical limits of what a given class of provider can verify are accounted for, rather than treating the obligation as uniform across all "operating systems."

GNI encourages ANPD to ensure that compliance approaches remain technologically neutral and achievable across providers of different sizes, so that the obligation does not unintentionally entrench the position of the largest firms.

III) Proportionality and the Risk Matrix

GNI appreciates the proportionality framework set out in the Guide, including that providers assess risks created by the assurance mechanism itself, not only by the underlying service. However, two aspects of the Risk Matrix, which categorises risk level based on service type, warrant attention.

The matrix lists biometric age estimation as an example mechanism in both the Moderate and High Risk tiers. Given the sensitive-data status of biometric processing under Brazilian Data Protection law, listing it as a standard example without qualification risks causing providers to treat it as an available default rather than a method of last resort. ANPD should state explicitly that biometric methods should be used only where non-biometric alternatives, including age signals, verifiable credentials, and document verification without facial matching, have been assessed as insufficient for the specific context. This would be consistent with the multi-layer model the Guide otherwise recommends.

Table 3 also places "general generative AI" in the Moderate Risk category as a single class. Generative AI products are widely diverse. A tool that answers a factual question in a single exchange does not carry the same risk as a companion-style chatbot designed for sustained, personal conversation with memory of the user across sessions. ANPD should either break "generative AI" into risk-based sub-categories, or state clearly that the Moderate Risk label is a starting point only, subject to the same case-by-case assessment the Guide already asks providers to apply to other services.

More broadly, proportionality requires not only that a chosen mechanism be suitable, but that it remain necessary in light of the rapidly changing socio-technical reality that applies to covered services. GNI encourages ANPD to clarify that providers should periodically evaluate whether an age assurance mechanism remains necessary and effective for the specific risks identified, and that where a less intrusive measure provides equivalent protection, providers should be encouraged to adopt it.

IV) Inclusion and Brazil's Socioeconomic Context

The Guide instructs that age assurance mechanisms account for the diversity of Brazilian socioeconomic contexts and avoid disproportionate exclusionary effects. UNICEF has previously found that Brazilian children on average have greater access to the internet than to housing, basic sanitation, or food security. Assurance methods that assume access to a smartphone with a reliable camera, stable broadband, or an official identity document may function as a meaningful access barrier for exactly the population the law is intended to protect and empower. ANPD should require that at least one available assurance pathway not depend on smartphone camera access, real-time video processing, sustained high-bandwidth connectivity, or possession of an official identity document, wherever the underlying service risk permits.

V) Accuracy, Robustness, and the Gap Between Example and Recommendation

The Guide includes an accuracy failure example, in which a 17-year-old user is misclassified into an uncertain age "gray zone" and sent for manual review with no defined timeline. The review takes seventy days, during which she turns 18, but because her case remains marked "under review," she stays locked out even after legally becoming an adult. The Guide describes this as a failure of accuracy and governance, but does not convert that finding into a binding recommendation. ANPD could close this gap and mitigate the likelihood of chilling effect in such cases, by requiring that providers using estimation methods with a defined uncertainty zone offer an expedited review or alternative verification pathway for users who fall within it, with a maximum resolution period disclosed in advance, and by requiring that access not be kept blocked, or be provisionally restored, where a user can be confirmed to have reached majority during a pending review, without requiring disproportionate additional data collection.

The same example points to a broader need for procedural safeguards wherever an assurance decision restricts access. GNI encourages ANPD to require that users receive meaningful notice when access is denied, an accessible route to contest the decision, and an explanation sufficient to understand it. Where an automated system determines access, a route to human review should be available. The Guide already references contestation and rectification rights, and stating these procedural expectations directly would give them operational effect.

VI) Privacy: Data Retention, Enforcement Capacity and Interoperability

GNI welcomes the Guide's treatment of data minimization, the prohibitions on secondary use, traceability, and the recommendation to use double-blind architectures and tokenized credentials. If implemented as written, this would represent a meaningfully privacy-protective model relative to age assurance regimes being adopted in other jurisdictions.

Data minimization obligations are also only as strong as the enforcement capacity behind them. ANPD should publish an enforcement and monitoring timeline alongside the final Guide, so that regulated entities and the public have visibility into how and when compliance with these privacy safeguards will be assessed, and do not cast a wider net than is necessary.

GNI welcomes the double-blind architecture in the Guide, under which a third-party verifier confirms a user's age without learning which app requested the check, while the requesting app receives only the age result. The Guide's statement that 'interoperability must not be confused with creating extensive integrated databases or permanent raw data transmission across firms is an important safeguard'.

GNI notes a tension between this principle and Section II, which requires providers in several contexts to verify age regardless of the age signal received, even where an app store or operating system has already performed reliable assurance upstream. This makes it unclear

how much independent re-verification a provider still owes after receiving a reliable signal, and risks undermining interoperability's privacy benefit if users face duplicative biometric or document checks at each layer. ANPD should clarify when a provider may rely on an upstream signal without re-verification, and when independent verification remains required notwithstanding a positive signal. GNI also encourages ANPD to clarify that participation in any shared or consortium-based credential scheme, such as the "V-Idade" example described in the Guide, should remain optional wherever a provider can meet its obligations through other compliant means, and that any such scheme remain open to independent civil society and academic review of how well it honors the double-blind model in practice.

Finally, GNI also warns against function creep. Age assurance systems introduced for the narrow purpose of distinguishing minors from adults should not evolve into broader identity or authentication infrastructure through later regulatory or commercial expansion. GNI further encourages ANPD to favor compatibility with established international interoperability standards where possible, so that providers operating across jurisdictions are not forced into fragmented, country-specific architectures that add cost and complexity without a corresponding privacy benefit.

Conclusion

ANPD has an important opportunity to ensure that the final Orientative Guide protects children and adolescents effectively while safeguarding the privacy and freedom of expression of all users. GNI commends ANPD for grounding the Guide in proportionality, necessity, and data minimization, and for the clarity of its privacy-protective default architecture. As drafted, gaps in the treatment of adult impact, scope, biometric defaults, accuracy safeguards, data retention, and centralization risk leave room for the Guide's strong underlying principles to be undermined in implementation. GNI encourages ANPD to consider the following recommendations:

- Treat impact on adult users, including chilling effects on lawful expression and the security risks created by assurance mechanisms themselves, as a standalone factor in the proportionality assessment, not only as a downstream data protection concern.
- Clarify how proportionality and risk-based principles apply to providers of general-purpose infrastructure, including operating systems, that may have limited practical ability to perform reliable age assurance.
- State explicitly that biometric methods are a last resort within each risk tier, not a default example.
- Sub-categorize generative AI services by actual risk characteristics, rather than classifying the category as a whole.
- Require at least one assurance pathway that does not depend on smartphone camera access, broadband connectivity, or possession of an official identity document, given Brazil's socioeconomic context.
- Require an expedited review pathway and maximum resolution period for users caught in an accuracy buffer zone, consistent with the Guide's own example.

- Confirm that metadata-only retention satisfies the auditability requirement under Section III.5, and publish an enforcement and monitoring timeline for the Guide's privacy safeguards.
- Keep participation in shared credential infrastructure optional and subject to independent civil society and academic review.

GNI is keen to engage further with ANPD throughout this consultation and welcomes opportunities to share GNI's multistakeholder perspective in support of a rights-respecting final Guide.