Age assurance mechanisms: proportionality, data minimization, and governance

Authors:

Beatriz Fazan

| Attorney in the Data Governance team at b/luz

Thiago Xavier Peregrino

| Attorney in the Data Governance team at b/luz

Reviewers:

Felipe Gabriades

| Partner in the Data Governance team at b/luz

Fernando Bousso

| Coordinating Partner of the Technology, Data Governance, and Media & Entertainment teams at b/luz

b/luz

b/luz

Summary

Introduction

The protection of children and adolescents in digital environments has been gaining increasing relevance in Brazil. As discussed in our most recent material on the topic, the enactment of Law No. 15,211/2025 (Digital Statute for Children and Adolescents, or "Digital ECA") consolidated certain relevant points regarding measures aimed at safeguarding the best interests of children and adolescents on the internet. The entry into force of the Digital ECA and the publication of Decree No. 12,880/2026 ("Implementing Decree") on March 17 and 18, 2026, respectively, indicate the need for discussion of key terms of the regulation. In this material, we will focus on age assurance mechanisms.

For the purpose of terminological clarity, we will adopt the definitions set forth in the Implementing Decree and by the ANPD[1], treating "age assurance" as a general term encompassing procedures intended to verify, estimate, or infer, directly or indirectly, a user's age or age range through different methods and technologies; and "age verification" as a specific form of assurance, characterized by the confirmation of age or age range based on direct evidence. Estimation and inference, in turn, operate by approximation or indirect deduction based on biometric, behavioral, or contextual data.

At the end of this material, we present two complementary annexes: Annex I, containing a summary of the next steps for companies in the context explored here, and Annex II, containing a structured guide for evaluating age assurance mechanisms, consolidating the criteria discussed throughout the text. It is important to note, however, that age assurance mechanisms represent only one of the regulatory pillars introduced by the Digital ECA, as the statute also addresses other relevant fronts aimed at protecting children and adolescents in the digital environment, such as parental control measures, safe design, and limitations on the offering of certain content and functionalities.

Restricting children's and adolescents' access to inappropriate situations follows the same logic that exists in the offline world. To ensure that only adults may participate in certain contexts, barriers must be established to access certain places, content, or products. In the digital world, these barriers take the form of what are known as age assurance mechanisms. There are various possible ways to verify the age of users online, unlike in the physical world, where, in general, verification is limited to checking identity documents.

1 BRAZIL. National Data Protection Agency. **Technological Radar 5 – Age Assurance Mechanisms**, Version 1.0. Brasília, DF, 2025. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf/view. Accessed on April 20, 2026.

In a scenario where people that are usually responsible for carrying out age assurance are replaced by software, APIs, and companies, these mechanisms bring with them concerns regarding the protection of the personal data collected for age assurance. Unlike a person, who has a relatively limited capacity to store information and a reduced possibility of later using the personal data that was checked, such as name, taxpayer ID number, and date of birth, technological systems have a virtually unlimited capacity to store this information and reuse it for subsequent purposes, which often depends on simple settings. For this reason, when we think about the digital environment, privacy and surveillance concerns become more acute.

The next section will explore the principles that guide the implementation of age assurance mechanisms, as indicated by the Digital ECA and the Implementing Decree.

1. Principles for adopting age assurance solutions

Before moving forward with the analysis of age assurance mechanisms, it is important to note that the ANPD, in its preliminary guidance[2], structures the issue around six fundamental requirements that should guide the implementation of these solutions:

Proportionality	The mechanism adopted must be compatible with the service's level of risk, avoiding solutions that are either insufficient or excessively intrusive.
Accuracy, robustness, and reliability	This refers to the degree of precision with which the mechanism can correctly identify the user's age or age group, the system's ability to withstand fraud attempts, and the consistency of results over time and across different contexts of use.
Privacy and personal data protection	Age assessment must be carried out using the minimum amount of data possible, with appropriate security measures and safeguards against improper use, in line with the principles of the LGPD.
Inclusion and non-discrimination	The mechanisms must not create disproportionate barriers to access or generate discriminatory effects across different groups.
Transparency and auditability	The processes must be understandable to users and subject to inspection, including by authorities and independent third parties.
Interoperability	Different systems must be able to communicate securely and efficiently, avoiding redundancies and reducing the need for repeated data collection.

2 BRAZIL. National Data Protection Agency. **Reliable age assurance mechanisms: preliminary guidance**. Version 1.0. Brasília, DF, 2026. Available at: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/view. Accessed on April 6, 2026.

2. Current debate: the most relevant mechanisms

Age assurance mechanisms have evolved alongside the development of digital technologies and the growing sophistication of data-driven business models. Today, they can be grouped into different categories, each with its own characteristics, distinct levels of reliability, and different impacts from a personal data protection perspective.

Below, we discuss examples of mechanisms that are already recognized, including possible use cases within the digital environment.

2.1. Self-declaration and declaratory mechanisms

The simplest and historically most widespread form of age assurance consists of user self-declaration, usually implemented through a field for entering a date of birth or confirming legal age (such as a button stating “I declare that I am over 18 years old”).

This is a low-friction mechanism in the user interaction journey and involves relatively low cost. However, its effectiveness is limited, since it depends exclusively on the truthfulness of the information provided by the user, without any additional element of validation.

Consistent with what is already set out in the Digital ECA, the Implementing Decree reiterates that self-declaration does not constitute a valid age assurance mechanism, prohibiting its use both for unlocking access and for completing transactions involving content, products, or services restricted to adults. The regulatory text requires the adoption of “effective” age assurance mechanisms, reinforcing that the user’s simple declaration may be insufficient.

> **Example 1 – User confirmation:** When accessing a page containing restricted content, the user sees a notice stating that the environment is intended only for individuals over 18 years of age. To proceed, the user must click a button stating, “I confirm that I am over 18 years old”. After the click, the system immediately grants access to the content. In this case, because access depends solely on information provided by the user, without any additional validation, this is a case of self-declaration.
>
> **Example 2 – Registration with CPF and date of birth:** During account creation, the platform requires the user to provide their CPF number and date of birth in mandatory fields. Based on the information entered, the system merely validates whether the CPF exists and uses the date of birth to determine whether the account may be created and which features will be available.
>
> Although the CPF is collected, the platform only validates its existence, without any consultation with or validation of the truthfulness of the date of birth against external databases, so the system treats the data provided by the user as true. Because the classification depends solely on information provided by the user, without any independent validation, this is a case of self-declaration.

2.2. Documentary verification

Another category of age assurance mechanisms is based on validating information against structured external sources associated with the user's civil identity. In such cases, age verification occurs, deriving from previously established data, such as the date of birth appearing on official documents or in reliable databases.

The most common example consists of submitting an identification document, such as an ID card or driver's license, by image capture or upload. Based on this information, the system extracts the data to confirm that the user is the same person as shown in the document provided and verifies the user's age information through the date of birth. This method works as an adaptation of physical document verification, as traditionally used to allow entry into certain establishments or enable the purchase of products intended for adults.

Compared with self-declaration, documentary verification significantly increases the level of security and reliability of the verification process. On the other hand, it involves the processing of a greater volume of personal data and the participation of third parties, which requires attention to issues such as necessity, data minimization, and security.

> **Example 3 – Document capture via camera:** During registration, the user is instructed to use the device's camera to photograph their identity document. The system provides guidance on how to position the document and automatically reads the data. The extracted date of birth is used to determine the user's age and allow the flow to continue. Because age assessment is based on data obtained from an official document presented by the user, this is a case of documentary verification.

2.3. Biometrics

Another relevant category comprises mechanisms based on the use of the user's biometric characteristics. Unlike documentary verification, these solutions operate based on the individual's own physical attributes and may be used both for identification purposes and for age estimation.

As will be explained below, biometric mechanisms may involve different levels of reliability depending on how they are implemented. While biometric comparison techniques are used for identity authentication, solutions based on inference are probabilistic in nature and generally less robust.

2.3.1. Biometrics with prior comparison

The first modality consists of the use of biometrics for identity validation through biometric recognition techniques, such as facial comparison. In these cases, biometrics are used to confirm that the individual undergoing the procedure matches an identity

that was previously provided, usually linked to a validated document or registration.

This approach is often used in combination with documentary verification mechanisms, in which the user submits an identity document and undergoes biometric capture, which is then compared with a previously recorded image. That image may have been obtained during the verification flow itself or may be stored in previously established databases. In this model, age assessment does not derive from the biometrics themselves, but rather from the information contained in the validated document or record. Biometrics therefore act as an authentication mechanism, ensuring that the user matches the holder of the previously verified identity.

This method arises, for example, in systems and platforms that require a higher level of precision in detecting and confirming the identity of the user attempting to access them, such as banking apps. In these cases, biometric data are collected to validate the user's identity, which should not be confused with age assurance. Where biometric data are used solely for the purpose of identifying the holder's age, it is recommended that such data be discarded after verification and not used to identify the user, unless strictly necessary.

2.3.2. Age inference based on biometric and behavioral signals

Another approach consists of estimating age based on inferences drawn from user characteristics, such as facial analysis for age estimation, voice patterns, or even browsing behavior, for example typing speed or content consumption history. The objective is to estimate the individual's probable age based on statistical models, without necessarily identifying the person in a direct manner. These models are developed from large datasets composed of thousands of images, audio samples, and behavioral records previously labeled with the users' respective ages. Accordingly, this approach does not depend on a previously validated identity, but rather on the inference of attributes from statistical models.

One of the main challenges of this approach is accuracy. In practical terms, accuracy refers to the probability that the system will correctly classify an individual within a relevant age range. This aspect is particularly critical at borderline ages.

Another sensitive point concerns the possibility of algorithmic discrimination. Age inference systems may perform unevenly across different population groups. For example, in the case of persons with disabilities, non-white persons, older individuals, or persons in situations of socioeconomic vulnerability, biometric or behavioral characteristics may diverge from the patterns found in the systems' training datasets and in the calculation of the statistical models, increasing the likelihood of incorrect classifications.

In addition, mechanisms based on behavioral signals assume that the device being used is intended for individual use, reflecting consistent patterns from a single user. However, in scenarios involving limited access and shared use of access terminals,

the patterns collected may compromise the reliability of the inferences made. In this context, the implementation of mechanisms for contesting and reviewing automated decisions is especially relevant, allowing the user to challenge incorrect classifications and to have access to reasonable alternatives for proving their age.

It is worth noting that, in addition to the methods currently implemented more broadly in connection with biometric assurance, other methodologies are emerging based on new scientific studies and technological advances. For example, in the international context there are companies[3] that offer age assurance technologies based on a data subject's hand movement and physiognomy[4]. These promising technologies are still recent and, therefore, there is not yet widespread evidence regarding their effectiveness and feasibility.

Example 4 – Facial comparison with document: During the verification process, the user is asked to submit an image of an identity document and then perform a facial capture. The system compares the captured image with the photo appearing on the submitted document. Once a match between the images is confirmed, the date of birth shown on the document is used to verify the user's age. Because biometrics are used together with the document to confirm that the individual is the holder of the presented identity, and age derives from the information contained in the validated document, this is biometric identification combined with documentary verification.

Example 5 – Age estimation through facial analysis: When accessing a given functionality, the user authorizes the use of the device's camera. The system captures an image of the face and applies a facial analysis model to estimate the individual's probable age. Based on the estimate generated, the system classifies the user within an age range and allows or restricts access. Because age assurance occurs directly through the analysis of biometric characteristics, without the use of a document or external database, this is age estimation inference through biometric analysis.

Example 6 – Age assurance through behavioral profiling: A user who is already logged into a given network undergoes age assurance through automated technology based on their platform usage behavior. The profiles the user follows, how they interact with other users, their typing speed, and their posts determine, based on comparison with a database of other users, whether their behavioral profile is compatible with that of an adult user. Because behavioral data are used to indicate the user's age, this is age assurance based on behavioral signals.

2.4. Age assurance through the use of payment methods

It is also possible to mention mechanisms based on the authentication of payment methods. In such cases, the use of financial instruments, such as credit cards, functions as an indirect indicator of adulthood, based on the presumption that a user who has their own payment method is of legal age.

This mechanism may also be understood as evidence of parental or guardian supervision or consent, since even if a minor has access to a parent's or guardian's payment method,

3 MCCONVEY, J. **BorderAge promises 100% anonymous age assurance with hand gesture modality**. Biometric Update. Web, 2026. Available at: <https://www.biometricupdate.com/202501/borderage-promises-100-anonymous-age-assurance-with-hand-gesture-modality>. Accessed on April 9, 2026.

4 ABDERRAHMANE, M. et al. **Human Age Prediction Based on Hand Image using Multiclass Classification**. International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy. Bahrain, 2020. Available at: <https://www.researchgate.net/publication/348637921_Human_Age_Prediction_Based_on_Hand_Image_using_Multiclass_Classification>. Accessed on April 9, 2026.

there is a presumption that they are aware of the minor's expenditures. This type of solution is frequently adopted in paid digital services as a way of introducing an additional layer of access control, although it is criticized due to the possibility of excluding more vulnerable segments of society, its lack of accuracy, and its potential for fraud.

> **Example 7 – Validation through a credit card:** To access certain content, the user must enter the details of a valid credit card. The system authorizes the payment method with the issuer, thereby validating the payment details entered. The existence of a valid financial instrument linked to the user is used to allow access to the functionality. As assurance relies on an external element associated with a financial instrument, this constitutes age assurance through a payment method.

2.5. Tokens, credentials, and cryptographic proofs of age

More recently, solutions have emerged based on digital credentials and cryptographic mechanisms that make it possible to prove attributes, such as "being over 18 years old," while, in theory, limiting the sharing of personal data. Although widely discussed at the theoretical level and in international initiatives, these models still have limited practical adoption in the market, especially in large-scale applications.

These include models based on zero-knowledge proofs ("ZKPs"), and double-blind architectures. Broadly speaking, ZKPs allow a user to prove the truthfulness of a piece of information without disclosing any underlying data. Double-blind models, in turn, structure the interaction in such a way that none of the parties involved has full visibility over the transaction: the credential issuer does not know where the credential will be used, and the service provider does not have access to the user's identity.

Although both models are primarily aimed at preserving privacy, there are relevant distinctions between them. ZKPs are a specific cryptographic mechanism that enables proof without disclosure, whereas double-blind refers to an information flow architecture, which may or may not incorporate techniques such as ZKPs to strengthen guarantees of non-traceability. Taken together, these approaches seek to ensure that only the necessary attribute is shared, without exposing additional data.

However, implementation involves relevant challenges. From a technical and operational standpoint, these are complex and generally costly solutions, both in terms of development and integration with existing systems.

Another important point is that these models do not completely eliminate the need for prior identity or age assurance mechanisms. As a rule, the initial issuance of the credential or token depends on the use of other methods, such as documentary or biometric validation, to ensure that adult status has been correctly attributed to the user. The central difference lies in the architecture: once issued, the credential can be used separately from the original underlying data.

Example 8 – Issuance and use of a digital credential of legal age: Before accessing an age-restricted service, the user undergoes an age verification process with a trusted provider. In this flow, the user submits an image of an identity document and then performs a live facial capture, in accordance with the system's instructions. The captured image is compared with the photograph appearing on the document in order to confirm that the user is the holder of the presented identity. After the match is validated, the system extracts the date of birth from the document and confirms that the user meets the age of majority requirement. ***At this stage, there is documentary verification combined with biometric authentication through facial comparison.***

After validation, the provider issues a digital credential associated with the user, containing only the information necessary, such as confirmation that the user is over 18 years old, without including data such as name, CPF number, or date of birth. This credential is stored in a digital wallet or application under the user's control. ***At this stage, there is data minimization and separation between civil identity and the age-related attribute.***

When accessing an age-restricted service, the user presents the credential. The system requests only proof of the age-related attribute, without access to the original data used in the initial verification. ***At this stage, there is dissociation between the verified data and the shared data.***

Credential validation may occur through cryptographic protocols that make it possible to prove legal age without disclosing additional data. In this flow, the credential provider has no visibility into which service is being accessed, and the service has no access to the user's identity. ***At this stage, characteristics of cryptographic proofs and double-blind architecture can be observed.***

Because verification takes place based on a previously certified attribute, with limited information sharing and without exposing the user's identity, this is, in an overall analysis, a model based on digital credentials.

2.6. Testing environments and systemic integration in the digital ecosystem

Assurance mechanisms have also been incorporated into broader ecosystems, such as regulatory testing environments, or testbeds, and solutions integrated into digital infrastructures, such as government digital identities, digital wallets, and operating systems.

In this context, particular note should be made of the European Union's experience with the implementation of the European Digital Identity Wallet[5], which envisages an interoperable digital identity model under which users will be able to store and share verified attributes, including proof of age, selectively and securely. Although this method has been praised internationally, it presents challenges for adoption in Brazil, given the country's digital literacy gaps[6] and unequal internet access across different regions[7].

Under this logic, age assurance ceases to be an isolated functionality and instead becomes part of a broader architecture of identity and digital trust. This could allow for greater

5 EUROPEAN COMMISSION. **European Digital Identity Wallet**. Brussels, 2024. Available at: <https://digital-strategy.ec.europa.eu/en/factpages/european-digital-identity-wallet>. Accessed on April 9, 2026.

6 BRAZIL. National Telecommunications Agency. **Diagnostic Bulletin: Digital Skills in Brazil and Around the World**. Brasília, 2024. Available at: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbIGuBQv-TrV78dFpuB7IKQqoNrnZCOZ3jtE5kL3VAa5556cOPl5SUdQPc8loctKVzQanQNRvclh1XFEKYys8Yfr>. Accessed on April 9, 2026.

7 CNN. **More than 20 million Brazilians still have no access to the internet, says IBGE**. Web, 2026. Available at: <https://www.cnnbrasil.com.br/tecnologia/mais-de-20-milhoes-de-brasileiros-ainda-nao-tem-acesso-a-internet-diz-ibge/>. Accessed on April 9, 2026.

consistency in the application of age-related controls, as well as a potential reduction in redundancies in data collection.

On the other hand, these systems do not operate autonomously. Mechanisms integrated into the digital ecosystem depend on other assurance processes, such as documentary validation, biometric validation, or other robust methods, to ensure the reliability of the attributes that will later be shared. The innovation being tested therefore does not lie in eliminating these stages, but rather in the way they are organized and reused within an interoperable infrastructure.

2.7. Timing of age assurance in the user flow

In addition to the choice of mechanism, another relevant aspect concerns the point at which age assurance is carried out in the user interaction flow. Age assessment may take place at different stages, such as upon first access to the service, at the time of account creation, upon completion of a purchase or entry into specific areas of the platform.

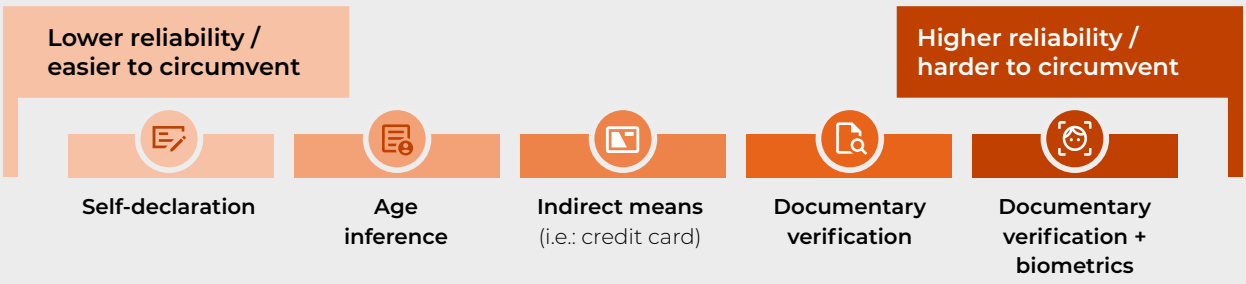
The definition of this timing directly affects the user experience, the level of friction in the service, and the effectiveness of the control implemented, and should be considered together with the level of risk associated with the activity.

2.8. Reliability of age assurance mechanisms

Age assurance mechanisms may be organized according to the degree of dependence on the information provided by the user, the existence of external validation, and the ability to withstand attempts at circumvention.

At one end are declaratory mechanisms, which depend exclusively on self-declaration. Next are models based on inference, which estimate age based on the user's characteristics. At intermediate levels are solutions that rely on indirect external elements, such as payment methods, as well as documentary verification mechanisms. At higher levels of reliability, particular note should be made of models that combine documentary verification with biometric authentication.

It is worth noting, however, that greater technical reliability does not automatically imply greater regulatory adequacy, and the choice of mechanism must therefore comply with the principle of proportionality.



3. Effectiveness and impact

The effectiveness of age assurance mechanisms must also take into account their impact on the user experience, including legitimate access to the internet. First, it is important to recognize that the effectiveness of a mechanism depends on its rate of adoption by users. In this sense, more stringent mechanisms may, paradoxically, be less effective if they create excessive barriers to use. A recent study conducted by Carnegie Mellon University[8] showed that more intrusive methods, such as the submission of an official document, had significantly lower completion rates (ranging from 17% to 28%), whereas simpler mechanisms, such as self-declaration, reached rates close to 99%. This shows that there is a structural tension between security and usability: the higher the level of stringency, the greater the user resistance tends to be.

This discussion must also be considered from the perspective of digital inequality. The complexity of technology may disproportionately affect certain groups, such as individuals with lower levels of digital literacy, limited access to devices, poor connectivity, or even documentary restrictions. Depending on the solution adopted, the assurance system may, in practice, create additional barriers for already vulnerable populations.

Considering this scenario, the definition of age assurance mechanisms under the Digital ECA requires an approach based on balancing different normative and practical factors, because overly permissive mechanisms are insufficient, but overly restrictive solutions may also fail. The challenge, therefore, lies in finding proportionate solutions that fulfill their purpose without creating new risks or discrimination in the digital environment, as will be further explored in the next section.

4. Proportionality as a structuring criterion

The analysis of age assurance mechanisms shows that there is no single solution capable of addressing all contexts of application. In this scenario, the principle of proportionality emerges as a structuring criterion for the interpretation and implementation of the obligations set out in the Digital ECA.

Proportionality may be understood as a criterion for calibrating age assurance measures in relation to the risks they are intended to mitigate. It therefore involves defining the most appropriate solution in light of the specific circumstances of each service or activity.

In practice, the application of proportionality may be guided by two central questions that should inform providers' decision-making:

8 LIN, Y., et al. **User (Non-)Compliance with Age Verification: Preliminary Evidence from a Deceptive Web Experiment.** Carnegie Mellon University CyLab Security and Privacy Institute. Pittsburgh, United States, 2026. Available at: https://www.cs.cmu.edu/~sscheffl/docs/2026/AgeVerif2026.pdf. Accessed on April 6, 2026.

PROPORTIONALITY	
What risks does the service or product pose to children and adolescents?	**What risks are associated with the age verification mechanism adopted?**
This analysis concerns the potential impacts of the digital environment itself, depending on the type of functionality made available.	Certain mechanisms may involve the processing of sensitive data, create barriers to access and risks of discrimination, and increase the likelihood of security incidents.

Proportionality therefore requires a combined analysis of these two risk vectors. For example, more intrusive mechanisms may be justifiable in contexts involving greater potential harm, but they tend to be disproportionate when applied to lower-risk services.

The proper application of the principle of proportionality is essential to avoid ineffective measures and the imposition of excessive burdens, ensuring that the Digital ECA produces effects compatible with the Brazilian reality.

In this context, it is relevant to recognize that the very logic of the Digital ECA reflects not only concern with risk mitigation, but also the broader objective of enabling a safe and accessible digital environment for all. This point is particularly relevant when one considers the central role that the internet plays. The digital environment is essential for access to information, education, culture, civic participation, and economic development. For children and adolescents, the internet may represent an important tool for learning, socialization, and inclusion. In this sense, the disproportionate limitation of access to the digital environment may deepen inequalities, restrict opportunities, and compromise the full development of individuals.

Thus, proportionality stands out as a central element for the implementation of solutions that are, at the same time, legally appropriate, technically feasible, and effective in protecting children and adolescents, without compromising safe and sustainable access to the digital environment. This logic of combined risk and proportionality analysis also guides the set of criteria consolidated in Annex II, which translates these elements into assessment parameters applicable to different contexts.

5. Data minimization and risks associated with age assurance

Article 24, paragraph 3, of the Implementing Decree[9] expressly prohibits the storage, retention, or any form of preservation of the image, the copy of the document, or the extracted information, all of which must be immediately and irreversibly deleted after the capture of the necessary data.

This limitation is especially relevant considering the nature of the data often involved in age assurance processes, which means that data minimization should not be restricted only to the collection stage, but must extend throughout the entire data processing lifecycle. The mechanisms adopted should prioritize solutions that reduce the amount of data processed and avoid retaining information after verification. In general, care should be taken to ensure that the control mechanisms themselves do not become autonomous sources of risk.

6. Governance as an essential element

The effective implementation of the obligations set out in the Digital ECA requires the structuring of governance models capable of supporting, documenting, and demonstrating the adequacy of the age assurance mechanisms adopted.

In this regard, the Digital ECA itself reinforces the centrality of governance by establishing the need to prepare formal assessment and monitoring instruments, such as impact reports, which must be available for sharing with the ANPD upon request.

In this context, governance allows agents to demonstrate not only that they have adopted protective measures, but also that these measures were chosen in a proportionate manner and are appropriate to the specific context of their activities.

Furthermore, the structuring of appropriate governance contributes not only to compliance with legal obligations, but also to building trust with users, regulators, and other stakeholders. In a context of growing scrutiny over digital practices, the ability to demonstrate responsibility and commitment to the protection of children and adolescents is likely to become a relevant differentiator. The structuring of these governance elements finds practical correspondence in the next steps suggested in Annex I, as well as in the assessment criteria consolidated in Annex II.

9 **Article 24, paragraph 3:** The processing of data resulting from the collection of documents must be limited to the data relating to age or confirmation of the age range, and the storage, retention, or any form of preservation of the image, the copy of the document, or the information is prohibited, and such data must be immediately and irreversibly deleted after the capture of the necessary information, pursuant to Law No. 13,709, of August 14, 2018.

7. Monitoring and enforcement timeline: gradual and risk-oriented implementation

The publication of the preliminary guidance by the ANPD was accompanied by the definition of a monitoring and enforcement timeline[10]. The regulatory strategy adopts a phased and predominantly preventive approach, initially focused on understanding the technical and operational challenges faced by regulated entities.

The ANPD's enforcement timeline may be understood in the following stages:

01 **Initial monitoring focused on structuring agents (immediate effect).**	The first phase, already underway, prioritizes the monitoring of app stores and operating systems, which are considered actors with a central role in the digital ecosystem. The choice of this group reflects a high-impact regulatory strategy: action aimed at a limited number of agents may generate relevant systemic effects for the protection of children and adolescents.
02 **Expansion of monitoring on a risk basis (starting in August 2026).**	At a second stage, scheduled for August 2026, the ANPD will expand the scope of enforcement to include other sectors. This expansion will be guided by criteria such as the level of risk associated with the services offered and the information collected during the initial phase.
03 **Regulatory consolidation and possible application of sanctions (subsequent stages).**	The timeline also provides for the updating of the enforcement and administrative sanctions regulations in order to align them with the new provisions of the Digital ECA, which is expected to take place from November 2026 onward. The beginning of enforcement actions is scheduled for January 2027.

It is relevant to note, however, that the establishment of a timeline by the ANPD does not prevent other bodies with enforcement powers, such as those focused on consumer protection, from independently initiating actions to assess the legal compliance of certain regulated actors, including the application of penalties in cases of noncompliance.

10 BRAZIL. National Data Protection Agency. **Decision Order CD/ANPD nº 35/2026**. Official Gazette of the Union. Brasília, 2026. Available at: <https://www.in.gov.br/en/web/dou/-/despacho-decisorio-cd/anpd-n-35/2026-694427648>. Accessed on April 6, 2026.

8. Final considerations

The implementation of age assurance mechanisms in the context of the Digital ECA represents a central aspect of the protection of children and adolescents in the digital environment. However, as demonstrated throughout this material, this is a topic that cannot be reduced to an isolated technical choice.

Age assurance should be understood as an element of risk-based governance, involving the integrated analysis of multiple factors. In this scenario, the adoption of proportionate approaches guided by data minimization is an essential tool for the design of sustainable solutions.

As a way of systematizing the discussions developed herein, Annexes I and II present, respectively, a set of next steps for companies and a guide for assessing age assurance mechanisms, allowing the practical application of the concepts of proportionality, minimization, and governance discussed here.

Ultimately, the challenge posed by the Digital ECA is not only to restrict improper access, but also to build a digital environment that is at the same time safe, accessible, and sustainable.

ANNEX I

Next steps for companies

In light of the entry into force of the Digital ECA and the publication of the ANPD's preliminary guidance, companies offering digital products or services accessible to children and adolescents should begin, or improve, their compliance processes based on a structured and multidisciplinary approach.

In this context, a number of practical steps stand out:

01	**Risk mapping and use cases**	Identify which products, functionalities, or user flows present potential risk to children and adolescents, taking into account aspects such as user interaction, access to sensitive content, and exposure to third parties.
02	**Assessment and selection of age assurance mechanisms**	Analyze the available age assurance mechanism alternatives in light of the criteria of proportionality, effectiveness, impact on user experience, and risks associated with the processing of personal data, avoiding standardized and decontextualized approaches.
03	**Review of personal data processing practices**	Ensure that the collection and use of data for age assessment are strictly limited to the specific purpose, with the implementation of data minimization, security, and data segregation measures.
04	**Structuring governance and documentation**	Develop policies indicating when and how impact reports, risk assessments, and other decision records should be produced to demonstrate the adequacy of the measures adopted, in line with the requirements of the Digital ECA and good data protection practices.
05	**Implementation of transparency and contestation mechanisms**	Ensure that users have access to clear information about how the mechanisms operate and are able to challenge automated decisions or incorrect classifications.
06	**Regulatory monitoring and continuous improvement**	Monitor the evolution of the ANPD's guidance and regulations and establish routines for the periodic review of the solutions adopted, taking into account technological advances and changes in the risk profile.

ANNEX II

Guide for the Assessment of Age Assurance Mechanisms

Based on the discussions developed throughout this material, we have compiled below the main assessment points that should be considered by companies when defining, implementing, or reviewing age assurance mechanisms.

This checklist reflects the ANPD's preliminary guidance and should be reviewed once final guidelines are published.

01. Proportionality and Risks

- ☑ **Product/Service Risks**: Have the potential adverse effects on the privacy, safety, and health of children and adolescents using the product been identified (i.e.: interaction between users or compulsive use)?
- ☑ **Mechanism Risks**: Has it been assessed whether the verification solution itself creates risks, such as the processing of sensitive data or the creation of undue barriers?
- ☑ **Balance**: Is the technical solution chosen proportionate to the level of risk of the service, balancing accuracy with privacy protection?
- ☑ **Supporting Instruments**: Has the preparation of a Data Protection Impact Assessment been considered?

02. Accuracy, Robustness, and Reliability

- ☑ **Accuracy Metrics**: Is the precision of the method in determining the relevant age range measured and periodically documented?
- ☑ **Fraud Resistance (Robustness)**: Has the system undergone testing to withstand attempts at circumvention or manipulation?
- ☑ **Data Sources (Reliability)**: Are the sources used reliable, independent, and robust? *Please note: pure self-declaration has a low degree of reliability.*

03. Privacy and Data Protection

- ☑ **Data Minimization**: Does the system process only the data or age-related attribute that is strictly necessary, avoiding the collection of unnecessary data?
- ☑ **Prohibition of Secondary Use**: Is it ensured that the data collected will not be used for purposes other than age assurance?

04. Transparency and Auditability

- **Clear Information**: Does the user receive information in simple and accessible language about the purpose of the verification and which data are used?
- **Contestation**: Is there an easy channel through which the user may challenge or rectify the result?
- **Audit Records (Logs)**: Does the company maintain records of operations without storing biometrics or document images for audit purposes?

05. Interoperability

- **Flow Security**: Are the limits of data flows, authorized agents, and safeguards against unrestricted sharing clearly defined?
- **Double-Blind Architecture**: Has the adoption of models been considered in which the verifier does not know the service provider, and vice versa, in order to enhance privacy?

b/luz

www.baptistaluz.com.br/