

Age Verification Technology S.L (AgeGO) – Public Practice Statement

About this Public Practice Statement

This Public Practice Statement provides a certified, informative summary of the Practice Statement identified by Age Assurance Provider Practice Statement Age Verification Technology SL v2 27.05.2026

The full Practice Statement and the underlying product, process or service has been assessed by the ACCS Certification Scheme and has met the applicable requirements of ACCS 1:2025 and ISO/IEC 27566-1:2025 - Age Assurance Systems - Part 1: Framework in accordance with scope of certification set out on their certificate and schedule.

The full Practice Statement contains sensitive, confidential or security-related information and is therefore not published. This public version provides information about the certified service while protecting information that should not be made publicly available.

For further information about the service, including enquiries about aspects of its operation that are not covered in this public summary, please contact the certified organisation directly.

Name of Client	Age Verification Technology S.L (AgeGO)
Public Practice Statement Title	Public Practice Statement
Public Practice Statement Version	1
Public Practice Statement Date	11.08.2026
Date Certified	3 rd June 2026

PUBLIC PRACTICE STATEMENT
Age Verification Technology, S.L. ("AgeGO")
Age Assurance Provider Practice Statement

1. Introduction and Purpose

Age Verification Technology, S.L. ("AgeGO") acts as an Age Assurance Provider (AAP), supplying age assurance results to relying parties. This Public Practice Statement provides the approach AgeGO takes to delivering age assurance services in line with applicable legal requirements and recognised technical standards, including the ISO/IEC 27566-1 framework.

2. Scope and Age Eligibility Outcome

AgeGO provides age assurance services to determine whether a user meets an "over 18" eligibility requirement. The outcome returned is binary: Verified (Over 18) or Not Verified. AgeGO does not currently offer configurable age thresholds (for example, over 16 or over 21).

Age-related eligibility requirements applied by AgeGO are set by: (i) the applicable laws and regulations of the relevant jurisdiction; and (ii) the relying party integrating AgeGO's services.

AgeGO acts as the age assurance provider and integrates third-party service providers as part of its verification processes.

3. Age Assurance Methods and Components

AgeGO offers users a choice of verification methods, built on independently certified third-party components:

- Selfie-based liveness detection and biometric age estimation.
- Identity document verification, combining document data extraction with facial matching against the document photograph.
- Digital identity verification through a trusted third-party identity provider.
- Credit card-based age inference, supported by additional payment authentication controls where available.

AgeGO applies its own decision logic to combine the outputs of these components and determine whether the required age threshold has been met. If verification cannot be completed successfully, no positive age assurance result is returned.

AgeGO's third-party components hold recognised independent certifications and attestations, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1, SOC 2, ISAE 3000 Type II, PCI DSS Level 1, BSI PAS 1296, and the UK Digital Identity and Attributes Trust Framework (UK DIATF).

Liveness detection and face matching components have additionally been independently tested by iBeta Quality Assurance, an accredited laboratory, in accordance with ISO/IEC 30107-3 (Presentation Attack Detection), demonstrating high accuracy and low error rates in production use.

4. Confidence and Effectiveness of the System

AgeGO applies conservative, internally defined confidence thresholds before returning a positive age assurance result, and offers alternative verification methods where a given method does not achieve sufficient confidence. Independent third-party testing of AgeGO's biometric components has demonstrated a high level of accuracy in both liveness detection and facial matching.

Where AgeGO relies on biometric age estimation, it applies an additional safety buffer above the legal age threshold and automatically escalates users to identity document verification where that buffer is not met.

AgeGO achieves the following per-method confidence levels: High for biometric age estimation (with a safety buffer and mandatory escalation to identity document verification); Very High for identity document verification and for digital identity verification; and Moderate for credit card-based authentication (used only in jurisdictions where strong customer authentication applies). Taken as a whole, AgeGO's integrated system — combining conservative threshold configuration, mandatory escalation logic, certified liveness detection, and identity-based verification — achieves a **Highly Effective level of assurance**, consistent with the Enhanced Level of Assurance defined in the IEEE Standard for Online Age Verification (2089.1).

Where required by applicable law, AgeGO makes at least two independent verification methods available, so that overall system effectiveness does not depend on any single method.

5. Binding of the Result to the Individual

AgeGO binds each age assurance outcome to the individual who completed the verification process through a combination of facial matching (where applicable), secure session management, and authentication of returning users (for example, through one-time passwords, passkeys, or supported federated sign-in methods). A positive result is only issued where the verification process has been completed successfully within a defined, secure session.

6. Privacy and Data Protection

AgeGO applies a privacy-by-design approach and complies with applicable data protection laws, including the GDPR, UK GDPR, and CCPA. Only the personal data strictly necessary to perform age verification is processed, and that data is used exclusively for that purpose.

AgeGO's automated decision-making produces a strictly binary outcome ("suitable/unsuitable") and does not generate profiles or inferences beyond that purpose. Data subjects may exercise their rights of access, rectification, and deletion, and may challenge a verification decision.

AgeGO's processing activities are documented internally (including through Records of Processing Activities and Data Protection Impact Assessments, as applicable), and AgeGO maintains internal procedures to assess, manage, and respond to any data security incident.

7. Accessibility and Ease of Use

AgeGO's verification journey is designed to be simple, inclusive, and appropriate for both adults and children. It offers a choice of verification methods, clear step-by-step guidance in plain language, and compatibility with desktop and mobile devices. AgeGO's interface follows the Web Content Accessibility Guidelines (WCAG) 2.1.

8. Security, Resilience and Anti-Circumvention Measures

AgeGO maintains a security programme covering secure system architecture, encrypted communications, access controls, continuous monitoring, and incident management, and conducts regular independent security assessments of its systems.

AgeGO also implements a combination of technical and procedural controls designed to reduce the risk that its age assurance results are circumvented, including through collaborative attempts.

AgeGO recognises that no age assurance system can fully eliminate deliberate cooperation between individuals; its objective is to make such attempts significantly more difficult, less scalable, and less

likely to succeed, and it reviews these controls on an ongoing basis as part of its security, compliance, and risk management processes.

9. Human Rights and Non-Discrimination Safeguards

AgeGO offers multiple verification methods, where technically and regulatorily feasible, so that no individual is systematically excluded due to lack of access to a particular document type, device, or payment instrument; where one method is not available to a user, an alternative is offered. The system is designed solely to determine whether a user meets the applicable age threshold, and does not restrict access beyond what is required for that determination, nor does it create profiles or draw inferences unrelated to age assurance.

Users receive clear, plain-language explanations of the verification process, including what data is collected and why, in a format accessible to both adults and children.

Where a user believes a verification outcome is incorrect, AgeGO provides a process to raise a concern and have the decision reviewed.

10. Governance, Audit and Continuous Review

AgeGO's Practice Statement and the underlying age assurance system are subject to continuous internal review, and are formally reviewed and approved by AgeGO's top management, which also ensures that adequate resources are allocated to maintain secure and compliant operations.

AgeGO's activities, systems, and this Practice Statement are subject to external audit, certification, and third-party review, as required by regulators or ecosystem stakeholders, in order to maintain the chain of trust across the age assurance ecosystem.