SafePassage Age Assurance — AGCOM Compliance One-Pager

Legal-readiness documentation for adult content platforms operating in Italy

---

Product Overview

SafePassage is a privacy-first, AI-powered age verification platform designed for regulated content platforms. It delivers real-time facial age estimation and ID-based verification with temporary image processing, to support assessment against AGCOM's Resolution No. 96/25/CONS implementing the Decreto Caivano.

Key Features:

- Dual verification modes: L1 (facial age estimation) and L2 (document verification with configurable biometric face matching)
- Temporary images; retained results and audit history
- - Age estimation and liveness checks; outcomes depend on capture conditions and deployment.
- Full liveness detection and spoof prevention
- Biometric face matching controlled by feature flag — can be disabled for Italian deployments
- - SDK integration with a hosted verification flow
- Real-time audit trails and stateless API architecture

Compliance Statement

SafePassage is designed to meet the requirements of AGCOM's Resolution No. 96/25/CONS, which mandates age verification for websites and video-sharing platforms distributing pornographic content in Italy. Our architecture and verification methods are aligned with AGCOM's eight mandatory principles: proportionality, personal data protection, cybersecurity, accuracy and effectiveness, accessibility and ease of use, inclusiveness and non-discrimination, user education and awareness, and effective complaint handling.

AGCOM explicitly excludes the processing of biometric data for the purpose of identifying or authenticating a natural person — including comparing an ID photograph with a selfie via facial recognition technology. SafePassage's biometric face matching is controlled by a feature flag and can be disabled for Italian deployments, ensuring the L2 escalation pathway relies on document authentication and liveness detection only.

AGCOM also requires platforms to offer at least one age verification system operating under double anonymity principles. Double anonymity is achieved through the combined operation of SafePassage and Emblem, VerityGuard's privacy tokenisation platform (see below).

AGCOM — SafePassage Compliance Summary

Requirement	Description	SafePassage Implementation
Proportionality	The method must be as non-invasive as possible to achieve the objective.	L1 uses a selfie for age estimation. Images are temporary for checks and retries; results and audit history may remain.
Data Protection	Must comply with GDPR. No profiling. No collection of identity, age, or personal information by involved parties. No facial recognition (selfie-to-ID matching).	Temporary image processing is separate from verification results and audit records. Verification methods must be configured for the deployment and applicable requirements.
Cybersecurity	Must include sufficient security measures to mitigate cyberattack risks.	Encrypted transport protects data in transit. Temporary verification images are separate from results and audit history. Operational controls support monitoring and audit review.
Accuracy & Effectiveness	Must contain errors in age determination. Performance measured by MAE, standard deviation, and false positive rate.	Age-estimation and liveness outcomes depend on capture conditions, the check and the complete deployment. Assess suitability using current, applicable performance evidence and configured thresholds.
Accessibility	Must be easy to use, designed with regard to minors' abilities.	L1 completes in seconds with any camera-equipped device. No account creation required. Clear step-by-step guidance for L2 if triggered.
Non-Discrimination	Must avoid discriminatory outcomes across demographic groups.	Assess demographic performance and potential bias using current evidence appropriate to the deployment. No universal accuracy or demographic-difference figure is asserted here.
User Education	Users must be informed about the verification process.	Current processing information is available in SafePassage's Privacy Policy and Biometric Information Disclosure. This document does not introduce an additional verification screen.
Complaint Handling	Users must have effective mechanisms to contest results.	Users can re-initiate verification. L2 document verification (with face matching configurable to be disabled) available as alternative pathway.
Independence	Provider must be legally and technically independent from content platforms.	Websites requesting checks receive the verification result, type of check and threshold. They do not receive verification images or details read from the ID.
Double Anonymity	Platforms must offer at least one system where the platform cannot identify the user and the provider cannot identify the destination site.	Requires deployment with Emblem (see below).

Double Anonymity — Emblem Integration

AGCOM mandates that content platforms offer users at least one age verification system operating under double anonymity principles (*doppio anonimato*). The platform must not be able to identify the user, and the verification provider must not know which site the user is accessing.

SafePassage alone satisfies platform-side anonymity — the platform receives only a cryptographic pass/fail token with no user-identifying data. However, verification-side anonymity — ensuring SafePassage cannot see which platform initiated the request — requires Emblem, VerityGuard's privacy tokenisation platform.

How it works:

1. The content platform initiates the verification request through Emblem.
2. Emblem strips the platform's identity — including its URL, domain, and any identifying metadata — before forwarding the request to SafePassage's age estimation engine.
3. SafePassage performs the age check without any knowledge of which content service the user is attempting to access, and returns the result to Emblem.
4. Emblem delivers a blockchain-anchored age token to the user.

No single party in the verification chain possesses sufficient information to both identify the user and determine which content service they are accessing.

Methods Excluded by AGCOM

Method	AGCOM Position	SafePassage Compliance
Credit card / mobile checks	Deemed weak; permitted only as secondary signals	Not used as a primary method
Email, social media, or SSO accounts	Not considered satisfactory	Not used
SPID / CIE (Italian government login)	Not compliant with double anonymity	Emblem's protocol-level separation prevents any component from seeing the destination site
Direct ID collection by content platform	Explicitly prohibited	Platforms never access identity data
Age estimation based on browsing history	Explicitly excluded	Not used
Biometric comparison between selfie and ID	Excluded as facial recognition technology	Biometric face matching can be turned off for Italian deployments; L1 uses age estimation only, L2 escalation relies on document

Method	AGCOM Position	SafePassage Compliance
photo		authentication and liveness without selfie-to-ID matching

This document is provided for informational purposes only and does not constitute legal advice. Regulatory interpretations may evolve. SafePassage makes no representations or warranties regarding legal outcomes. Please consult your legal counsel or contact SafePassage for the latest compliance documentation.