SafePassage Age Assurance — Arcom Compliance One-Pager

Legal-readiness documentation for adult content platforms operating in France

---

Product Overview

SafePassage is a privacy-first, AI-powered age verification platform designed for regulated content platforms. It delivers real-time facial estimation and ID-based verification with temporary image processing, to support assessment against Arcom's SREN framework and French legal requirements.

Key Features:

- Dual verification modes: L1 (facial estimation) and L2 (ID + biometric)
- 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
- - SDK integration with a hosted verification flow
- Real-time audit trails and stateless API architecture

Compliance Statement

SafePassage can support a deployment assessed against Arcom's technical age-verification framework. Suitability depends on the complete implementation, including effective adult access checks, an independent verification flow, privacy protection and audit evidence. Product capabilities alone do not establish validation of a deployment.

Arcom's référentiel requires that platforms offer users at least one age verification option that operates under double anonymity principles. Double anonymity is achieved through the combined operation of SafePassage and Emblem, VerityGuard's privacy tokenisation platform (see below).

Arcom — SafePassage Compliance Summary

Requirement	Description	SafePassage Implementation
Binding	Age verification outcome must be binding and tamper-proof.	Each verification session issues a signed, cryptographic token used by the platform to enforce access control.
Independence	Age verification must be performed by an independent, neutral provider.	SafePassage operates as a third-party service — platforms never access verification data and cannot override results.

Requirement	Description	SafePassage Implementation
Auditability	Regulator or platform must be able to verify that checks occurred.	Real-time webhook callbacks and immutable, signed session logs provide a full audit trail without exposing user data.
No PII Leakage	Verification process must not expose personal data to either the platform or the verification provider.	The platform never sees ID images or facial data. Double anonymity — ensuring SafePassage also cannot see the destination site — requires deployment with Emblem (see below).
Irreversible Outcome	The age-verification result must be final and not reusable for identifying the user elsewhere.	Tokens contain only a binary age-verified flag; no reusable identifiers or biometric templates are stored or returned.

Double Anonymity — Emblem Integration

Arcom requires platforms to offer at least one age verification method that complies with double anonymity: the content platform must not be able to identify the user, and the verification provider must not be able to identify the content service 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.

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.