SafePassage Age Assurance — GDPR Compliance One-Pager

Legal-readiness documentation for privacy and data-protection obligations under the EU General Data Protection Regulation (GDPR)

Product Overview

SafePassage is a privacy-first, AI-powered age verification platform designed for regulated content platforms. It delivers real-time facial estimation (L1) and document-plus-biometric verification (L2) while ensuring **full alignment with the General Data Protection Regulation (GDPR)**. SafePassage's architecture is built on **ephemeral processing** — no personal data is ever stored.

Key Features

- Dual verification modes: **L1** (facial estimation) and **L2** (ID + biometric match)
- **Zero PII retention** — all inputs deleted within milliseconds
- 99.7 % accuracy at 18+ threshold
- Full liveness detection and spoof prevention
- Compact size, installable in under 5 minutes
- Real-time audit trails and stateless API architecture

Compliance Statement

SafePassage is designed and operated in full conformity with the **EU General Data Protection Regulation (GDPR)**. Its architecture and operational controls meet or exceed GDPR requirements for lawfulness, fairness, transparency, data minimisation, purpose limitation, security, and user rights (including right to erasure and access). Since SafePassage **never stores personal data or biometric templates**, many GDPR obligations — such as breach notification and data subject requests — are simplified or not triggered.

GDPR — SafePassage Compliance Summary

GDPR Principle / Article	Summary Requirement	SafePassage Implementation
Lawfulness, Fairness & Transparency (Art. 5(1)(a))	Processing must be lawful, fair and transparent to users.	SafePassage provides clear privacy notices and processes only what is strictly necessary for age verification.
Purpose Limitation (Art. 5(1)(b))	Data collected must be used only for specified, legitimate purposes.	Age-verification data is used **solely** for real-time age assurance; no secondary uses or profiling.
Data Minimisation (Art. 5(1)(c))	Only data necessary for the stated purpose may be processed.	L1 requires only a live selfie; L2 requires ID and selfie just for instant verification.
Storage Limitation (Art. 5(1)(e))	Personal data must not be stored longer than necessary.	All biometric and ID data are processed **in-memory and deleted within milliseconds**.
Integrity & Confidentiality (Art. 5(1)(f) + Art. 32)	Data must be protected against unauthorised or unlawful processing.	Ephemeral caches; all data deleted within milliseconds, no PII data retained at all. SOC2-aligned operational controls.
Right to Erasure & Access (Art. 17 & 15)	Individuals can request deletion or access to their data.	No personal data retained; these rights are satisfied by design.
Accountability (Art. 5(2))	Controller must be able to demonstrate compliance.	Immutable, signed audit logs show that age checks occurred without retaining any PII.

Regulatory Contact Readiness

Full documentation — including Data Protection Impact Assessment (DPIA), security architecture, and GDPR legal analysis — is available to legal teams and supervisory authorities upon request. Materials are provided under NDA and include technical flow diagrams, privacy notices, and encryption key-management details.