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 provides facial age estimation and document-plus-biometric verification. Images are processed temporarily for checks and retries; results and audit records may be retained as service history. GDPR responsibilities depend on the deployment and the processing involved.

Key Features:

- Dual verification modes: L1 (facial estimation) and L2 (ID + biometric match)
- 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 supports age verification with temporary image processing. Verification results and audit records may remain in service history. GDPR obligations, including lawful processing, transparency, security and data-subject rights, apply according to the deployment and processing involved.

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.

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.	Temporary images for checks and retries; results and audit history may remain.
Integrity & Confidentiality (Art. 5(1)(f) + Art. 32)	Data must be protected against unauthorised or unlawful processing.	Encrypted transport and access controls protect service records.
Right to Erasure & Access (Art. 17 & 15)	Individuals can request deletion or access to their data.	Access and erasure requests are handled under the applicable service policy; retained records must be assessed by type.
Accountability (Art. 5(2))	Controller must be able to demonstrate compliance.	Verification results and audit records support service history and accountability; their retention is separate from temporary images.

Regulatory Contact Readiness

Contact SafePassage for current implementation documentation. A deployment assessment should cover its lawful basis, privacy notices, security, data-subject request handling and any required impact assessment.

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.