SafePassage Age Assurance — Ofcom Compliance One-Pager

Legal-readiness documentation for UK-regulated adult content platforms

---

Product Overview

SafePassage provides facial age estimation and ID-based verification with temporary image processing. Results and audit records may remain in service history. Deployment suitability must be assessed against Ofcom guidance; Ofcom does not approve individual age-assurance providers.

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

- Age estimation and liveness checks; outcomes depend on capture conditions and deployment.

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. Nothing in this document should be interpreted as indicating certification, endorsement, or rating by Ofcom or any other regulatory body. Please consult your legal counsel or contact SafePassage for the latest compliance documentation.

Ofcom — SafePassage Compliance Summary

Requirement	Summary Description	SafePassage Implementation
High Effectiveness	Must successfully prevent underage access with minimal false negatives.	L1 facial age estimation is a technology type identified by Ofcom as capable of being highly effective. L2 exceeds identity assurance thresholds.
Accuracy at Thresholds	Must reliably classify users at 18+ and 16+ age thresholds.	- Age estimation and liveness checks; outcomes depend on capture conditions and deployment.
Liveness Detection	Required to prevent spoofing via static images or video replays.	Sequential frame capture with motion analysis, spoof-resistance scoring, and session-level liveness verification.
Challenge Age Policy	Recommended to apply facial estimation at age 25 to ensure margin for error.	Challenge age set to 25 for UK deployments by default, configurable per integration.
Data Minimization & Privacy	Must avoid persistent biometric or PII storage.	Temporary images for checks and retries; results and audit history may remain.
Auditability	Must provide evidence that checks occurred without retaining user data.	Real-time webhook callbacks, signed session tokens, and audit logs.
No Self-Declaration	"Are you 18?" checkboxes and DOB fields alone are non-compliant.	SafePassage requires biometric verification or facial estimation for all age checks.

Regulatory Contact Readiness

Full documentation — including benchmark results, test environments, and integration guides — is available to legal teams and regulatory agencies upon request. Materials include flow schematics, liveness verification logs, and challenge-age configuration details.

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. Nothing in this document should be interpreted as indicating certification, endorsement, or rating by Ofcom or any other regulatory body. Please consult your legal counsel or contact SafePassage for the latest compliance documentation.