SafePassage Age Assurance — KJM Compliance One-Pager

Legal-readiness documentation for adult content platforms operating in Germany

Product Overview

SafePassage provides facial age estimation and document-plus-biometric verification using the underlying SafePassage technology. Images are processed temporarily for checks and retries; results and audit records may remain in service history. KJM assessment scope and implementation conditions are described below.

Key Features:

• Dual verification modes: L1 (facial age estimation) and L2 (document verification + biometric face match)
- Temporary images; retained results and audit history
- Age-estimation outcomes depend on capture conditions and deployment.
• Full liveness detection and spoof prevention
- KJM assessment condition: fixed five-year buffer (age 23 for an 18+ service)
- SDK integration with a hosted verification flow
• Real-time audit trails and stateless API architecture

Compliance Statement

SafePassage has received a formal positive assessment from the KJM for age verification of adult content services as set out in the JMStV (Jugendmedienschutz-Staatsvertrag). Both deployment models have been independently reviewed and approved:

• **SafePassage Module-Only Solution** — approved as a **Modul** (identification-level solution) implementing KJM's "one-time key" approach, requiring complete L1 age estimation (with automatic escalation to L2 document verification if inconclusive) for each session.

• **SafePassage + Emblem Master Key Solution** — approved as a **Gesamtkonzept** (full concept) implementing KJM's "master key" approach, combining rigorous initial L1/L2 identification with Emblem's secure token-based re-authentication for returning users.

KJM — Compliance Summary

Requirement	KJM Standard	SafePassage Implementation
KJM Positive Assessment	Providers must implement an age verification concept formally assessed and approved by KJM.	SafePassage has received a positive assessment from KJM for both Module-Only (Modul) and Master Key (Gesamtkonzept) deployment models, submitted under VerityGuard LLC.
Reliable Identification	The identification flow must meet the scope and conditions of the published KJM assessment. A complete deployment also requires suitable authentication.	Age estimation with the required fixed buffer and an ID fallback supports the assessed identification flow. Suitability depends on the complete implementation.
Challenge Age Threshold	KJM requires a 5-year buffer above the legal age threshold for age estimation systems.	The published KJM module assessment requires a fixed, non-adjustable five-year buffer above the legal age threshold: age 23 for an 18+ service.
Authentication (Master Key)	Master key solutions must prevent transfer of access credentials to minors through robust session-based authentication.	Emblem implements soul-bound (non-transferable) blockchain tokens on Polygon, multi-factor authentication (SMS OTP or FaceID/TouchID), and 5-minute inactivity timeouts requiring complete re-authentication.
Liveness / Anti-Spoofing	System must prevent spoofing through photos, video replays, or other manipulation.	Sequential-frame motion analysis, AI-powered spoof-resistance scoring, and session-level liveness verification built into the verification pipeline.
Data Protection & Privacy	Compliance with German and EU data protection law (GDPR). No unnecessary storage of personal data.	Temporary images for checks and retries; results and audit history may remain.

Requirement	KJM Standard	SafePassage Implementation
Auditability & Documentation	Providers must demonstrate to KJM that checks occurred and standards are met.	Real-time webhook callbacks and immutable, signed session logs provide a complete audit trail without retaining user images or ID copies.
Technical & Organisational Measures	Secure processing environment and controlled access to verification infrastructure.	Encrypted transport and access controls protect service records.

Deployment Models

Module-Only (One-Time Key)

The standalone SafePassage module requires complete verification for each session. The platform redirects the user to SafePassage, which performs L1 facial age estimation. If the user's estimated age is below the 23-year challenge threshold, the system automatically escalates to L2 document verification. A single-use confirmation is returned to the platform. No persistent tokens are issued between sessions.

SafePassage + Emblem (Master Key)

The integrated SafePassage + Emblem solution combines rigorous initial identification with secure re-authentication for returning users. First-time users go through the full L1/L2 verification. Upon successful verification, the user may create a master key account. Emblem deploys a soul-bound (non-transferable) token on the Polygon blockchain and registers the user's mobile number. Returning users authenticate via SMS OTP or biometric confirmation (FaceID/TouchID) at the start of each session, with 5-minute inactivity timeouts requiring complete re-authentication.

Double Anonymity

When deployed with Emblem, the SafePassage + Emblem Master Key solution implements double anonymity between the verification provider and the content platform. Emblem serves as a privacy intermediary: verification requests forwarded to SafePassage contain no information about which site the user is accessing, and the content platform receives only a binary 18+ confirmation without access to biometric data, identification information, or verification methodology details.

Regulatory Contact Readiness

Full documentation — including KJM positive assessment confirmation, benchmark results, and integration guides — is available to legal teams and regulatory agencies upon request. Materials include flow diagrams, liveness verification logs, and One-Time Key / Master Key deployment 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. Please consult your legal counsel or contact SafePassage for the latest compliance documentation.