

# SafePassage Age Assurance — KJM Compliance One-Pager

Legal-readiness documentation for adult content platforms operating in Germany

## Product Overview

SafePassage is a privacy-first, AI-powered age verification platform designed for regulated content platforms. It delivers real-time facial age estimation (L1) and document-plus-biometric verification (L2) with no data storage, and is fully compliant with the requirements of the Kommission für Jugendmedienschutz (KJM) under the German Interstate Treaty on the Protection of Minors in the Media (JMStV).

### Key Features:

- Dual verification modes: L1 (facial age estimation) and L2 (document verification + biometric face match)
- Zero PII retention — all inputs deleted within milliseconds
- 98.9% accuracy in correctly identifying minors (100% for ages 8–15, 95.8% for ages 16–17)
- Full liveness detection and spoof prevention
- Challenge age of 23 (5-year buffer above the 18+ legal threshold), meeting KJM requirements
- Compact size, installable in under 5 minutes
- 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                                                                                                                                                                                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>KJM Positive Assessment</b>       | 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.                                                                                                   |
| <b>Reliable Identification</b>       | Verification must securely confirm that the user is over 18. Master key solutions require reliability equivalent to face-to-face identification (≥95% accuracy). | L1 AI-powered age estimation achieves 98.9% accuracy for identifying minors, exceeding KJM's ≥95% reliability threshold. When estimation is inconclusive, automatic escalation to L2 document verification with ID capture, biometric face match, and liveness detection. |
| <b>Challenge Age Threshold</b>       | KJM requires a 5-year buffer above the legal age threshold for age estimation systems.                                                                           | Challenge age set to 23 for German deployments (5-year buffer above the 18+ threshold), providing 95.8% accuracy for 16–17 year olds and 100% accuracy for ages 8–15.                                                                                                     |
| <b>Authentication (Master Key)</b>   | 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.                                                             |
| <b>Liveness / Anti-Spoofing</b>      | 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.                                                                                                                      |
| <b>Data Protection &amp; Privacy</b> | Compliance with German and EU data protection law (GDPR). No unnecessary storage of personal data.                                                               | Zero PII retention — all biometric and document data processed ephemerally in memory and deleted within milliseconds. No persistent storage. End-to-end encryption (TLS 1.3 / AES-256-GCM).                                                                               |

| Requirement                                    | KJM Standard                                                                        | SafePassage Implementation                                                                                                                |
|------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auditability &amp; Documentation</b>        | 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. |
| <b>Technical &amp; Organisational Measures</b> | Secure processing environment and controlled access to verification infrastructure. | Stateless microservice architecture with TLS 1.3, AES-256-GCM encryption, and SOC 2-aligned operational controls.                         |

## 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.*