



Security & Compliance

sportpass.digital Plattform



Funktionen Sicherheit Preise Kontakt

🌟 Demo anfragen

🌟 Kontakt aufnehmen

• Für Verbände, Vereine & Mitglieder

Schluss mit Papierpässen. Sportpässe **digital & validierbar.**

Verwaltung, Freigabe und QR-Validierung in einer Plattform –
sauberer Workflow, klare Rollen, DSGVO-konform minimal
öffentlich.

QR-Validierung

Entwurf – Genehmigt – Freigegeben

Einladungen per Link

Passfoto (nicht öffentlich)

🌟 Kontakt aufnehmen

Funktionen ansehen

Öffentlich
Nur Status & Zeitstempel

Sicherheit
Rollen + Verbands Isolation



Ben Wegerle
Dein Sportverband

APPROVED

Sportart
Deine.Sportart

Verband
Dein.Sportverband

Gültig
Legitim

Freigabe
Zeitstempel

QR-Validierung

Read-only



Scan zeigt nur **Status, Sport, Verband** und **Freigabezeitpunkt** –
keine Personendaten.

Für Vereine & Verbände
Strukturierte Freigaben & Monitoring



1. Architekturüberblick

sportpass.digital ist eine webbasierte SaaS-Plattform zur Verwaltung und Validierung digitaler Sportpässe für Sportverbände.

Systemkomponenten: - WebApp Frontend - Backend (API) - PostgreSQL Datenbank - Objektstorage für Passfotos - Public Validation Service

2. Authentifizierung

Login erfolgt über Magic-Link E-Mail-Authentifizierung mit kurzlebigen Access Tokens und Refresh Token Rotation.

3. Rollen & Zugriffskontrolle

Rollenmodell: - App-Admin - Verband - Verein - Mitglied

Zugriffe sind rollenbasiert und mandantengetrennt organisiert.

4. Mandantenisolierung

Jeder Verband wird über eine eigene Subdomain isoliert (z. B. <https://{verband}.sportpass.app>).

Datenzugriffe werden serverseitig nach Federation-ID gefiltert.

5. Datenschutz

Öffentliche Validierung zeigt ausschließlich: - Sportpass-ID - Sportart - Verband - Status - Freigabezeitpunkt

Es werden keine personenbezogenen Daten öffentlich angezeigt.

6. Datensicherheit

Sicherheitsmaßnahmen: - TLS-verschlüsselte Kommunikation - Rollenbasierte Zugriffskontrolle - Tokenbasierte Sessions - Sichere Token-Generierung

7. Datenspeicherung

Personenbezogene Daten werden in einer PostgreSQL Datenbank gespeichert. Passfotos werden in einem Object Storage (z. B. S3) abgelegt. Regelmäßige Backups werden durchgeführt.

8. Monitoring

Das System verwendet strukturierte Logs, Request-ID Tracking und Monitoring-Events zur Sicherstellung der Systemstabilität.

9. Schutz der Public Validation

Die öffentliche Validierung ist geschützt durch: - nicht erratbare Tokens - Rate Limiting - Caching

10. Weiterentwicklung

Die Plattform wird kontinuierlich weiterentwickelt unter Einhaltung der Datenschutz- und Sicherheitsanforderungen.