Evaluator-Guide

Fachapplikation Arbeitsmarktvollzug (AMV)

Amt fuer Wirtschaft und Arbeit, Kanton St. Gallen

STAND	VERSION	STATUS
April 2026	1.3	Technisch freigegeben fuer Demo/Evaluation

DEMO-UMGEBUNG

Tour-Seite und HERMES-Dokumente auf der Demo-Umgebung verfuegbar

Zugang auf Anfrage - 17 HERMES-Dokumente verlinkt

1 Kurz und buendig

- ✓ Demo-Umgebung mit allen Kern-Features oeffentlich erreichbar (Zugang auf Anfrage).
- ✓ Tour-Seite unter `/tour` mit Screenshots aller Kern-Features (kein Login noetig).
- ✓ Alle 27 Compliance-Anforderungen aus Pflichtenheft Paragraf 5-7 sind technisch umgesetzt.
- ✓ Alle 8 externen Schnittstellen sind implementiert und vom Admin selbst konfigurierbar (Demo-Modus).

27 / 27	8	4	17
COMPLIANCE-ANFORDERUNGEN	SCHNITTSTELLEN IMPLEMENTIERT	VOLLZUGSBEREICHE	HERMES-DOKUMENTE

2 Zugangsdaten Testsystem

ROLLE	E-MAIL	BESCHREIBUNG
SYSTEM-ADMIN	`john@doe.com`	Volle Rechte: Audit-Log, Benutzerverwaltung, Retention
SACHBEARBEITER	`mueller@sg.ch`	Bearbeitet Faelle im eigenen Vollzugsbereich

Passwoerter werden separat kommuniziert. Weitere Test-Accounts werden auf Anfrage bereitgestellt.

3 Vollzugsbereiche und Aktenzeichen

Die Applikation deckt alle vier Vollzugsbereiche des AWA ab. Jedes Verfahren traegt ein eindeutiges Aktenzeichen `SG-JJJJ-NNNN-VB`.

VOLLZUGSBEREICH	SUFFIX	RECHTSGRUNDLAGE / INHALT
FlaM **FlaM - Schwarzarbeit i. e. S.**	`SCHW`	EntsG, BGSA. Lohnkontrollen, Bussen.
AIG **Auslaender und Integration**	`AIG`	AIG. Bewilligungen 18-120 Tage, Meldeverfahren.
BGSA **Bundesgesetz Schwarzarbeit**	`BGSA`	Register, Sanktionen, BV-Beitraege.
VA **VA / Fluechtlinge / S**	`VA`	Erwerbstaetigkeits-Bewilligungen.

4 Empfohlener Pruefpfad

20 MINUTEN

1. **Dashboard** - KPI-Kacheln pro Vollzugsbereich, Schnellaktionen, Workflow-Status. `/dashboard`
2. **Meldungen-Pipeline** - Kanban-Board, Filter `?filter=overdue` zeigt BGSA-konform nur ueberfaellige Faelle. `/meldungen`
3. **Meldung in Verfahren konvertieren** - Button im Meldungs-Detail erzeugt Aktenzeichen automatisch.
4. **Fall-Detail** - Dokumenten-Upload (S3, verschluesselt), Zeitachse, State-Machine-Transitions, Tab Schnittstellen fuer kontextbezogene Operationen. `/cases`
5. **PDF-Verfuegungen** - Tab Dokumente, Vorlagen mit Platzhaltern, Generierung ueber HTML2PDF-API.
6. **Schnittstellen-Konsole** - Endpoint, Credentials und Zertifikate pflegen, Verbindungstest pro Schnittstelle. `/admin/settings`
7. **Health-Check** - sechs Statuspruefungen in Echtzeit. `/admin/health`
8. **Tenant-Sicherheit** - TOTP-Pflicht, Bildschirmsperre, Sitzungsdauer pro Mandant. `/admin/security`
9. **Audit-Log mit Diff** - alle Mutationen mit Filter und Vorher/Nachher-Vergleich. `/admin/audit-log`
10. **Globale Suche** - Cmd+K, Volltext ueber Faelle, Personen, Firmen.
11. **Retention-Konsole** - DeletionPolicy pro Vollzugsbereich, manueller Trigger. `/admin/deletion-policies`
12. **Tour-Seite** - public mit allen Features als Screenshot-Sammlung. `/tour` - neu mit Sektion `#operations` fuer das Sicherheits-Cockpit.

5 Compliance und Sicherheit

DSG-Konformitaet

Region-Guard validiert beim Start, dass Storage in der freigegebenen Region liegt. Die aktuelle Umgebung dient Demo/Evaluation. Der produktive Betrieb erfolgt in einer vertraglich festgelegten Hosting-Region.

Authentifizierung

NextAuth.js, 2FA via TOTP (umschaltbar pro Tenant), Account-Lockout, Passwort-Historie 10 Generationen.

Audit-Log mit Diff

Prisma-Audit-Extension auf allen Writes. Vorher/Nachher-Vergleich pro Eintrag, AuditLog-Modell unveraenderbar.

Soft-Delete

Alle Faelle mit `deletedAt`. Physische Loeschung erst nach Karenz-Frist.

Schutzbedarf

ISDS klassifiziert als bedeutend (Stufe 2 von 3). PII-Felder AES-256-GCM verschluesselt, ueber Blind-Index suchbar.

Backup und Restore

PostgreSQL taeglich (30 Tage), S3-Versioning (90 Tage), Point-in-Time-Recovery unter 4h.

5a Sicherheits- und Betriebs-Cockpit

NEU IN APRIL 2026

Ergaenzungen aus dem aktuellen Hardening-Sprint. Alle Features sind im System aktiv, fuer Admins ueber das Menue erreichbar und auf der Tour-Seite (`/tour#operations`) dokumentiert.

Health-Check (`/admin/health`)

Sechs Pruefungen in Echtzeit: Datenbank, Storage, PII-Schluessel, Audit-Trail, Heartbeat, Region-Guard. JSON-Endpoint fuer Monitoring.

Tenant-Sicherheit (`/admin/security`)

Pro Mandant einstellbar: TOTP-Pflicht fuer Admins, Bildschirmsperre, Sitzungs-Lebensdauer. Alle Aenderungen audit-loggt.

Idle-Lock (Bildschirmsperre)

Sperrt das UI nach n Minuten Inaktivitaet (0..120). Passwort-Verifikation via bcrypt entsperrt ohne neuen Login. Fuer Mehrpersonen-Bueros.

Audit-Diff

Jeder Audit-Eintrag zeigt vorher/nachher-Werte als JSON-Patch. Filter nach Mandant, Aktion, Ressource, Zeitraum. Export als CSV.

PII-Adresse verschluesselt

Strasse, PLZ, Ort von Personen werden mit AES-256-GCM verschluesselt gespeichert. Suche ueber SHA-256 Blind-Index moeglich. Kein Klartext in der DB.

eIAM/AGOV SSO (technisch vorbereitet)

Vorbereitete Schnittstelle in `/admin/sso` . eIAM/AGOV technisch vorbereitet; Live-Anbindung und externe Abnahme erfolgen im Onboarding.

6 Stand der 8 Schnittstellen

IMPLEMENTIERT

Alle 8 Schnittstellen sind in der Applikation implementiert. Endpoint, Credentials und Zertifikate werden vom Admin in `/admin/settings` gepflegt. Im Demo-Modus laufen alle Schnittstellen mit Mock-Antworten. Produktive Aktivierung erfolgt nach kundenseitiger Konfiguration und Schnittstellenabnahme.

SCHNITTSTELLE	OWNER	AUTH-VERFAHREN	ZWECK
SECO ALV Taggeldstatus	SECO	OAuth2 Bearer	Echtzeit-Abfrage Taggeldstatus Arbeitslosenversicherung
ZEMIS Auslaenderdossier	SEM (sedex)	mTLS Client-Cert	Personen, Bewilligungen, Einreisen, Aufenthaltsstatus
SIMIC Auslaenderregister	SEM (sedex)	mTLS Client-Cert	Personenabgleich AIG / VA mit zentralem Auslaenderregister
FlaM-Plattform	SECO FlaM	OAuth2 Client Cred.	Kontroll-Export, Abgleich Arbeitgeberliste, Meldungen
AVAM Arbeitsvermittlung	SECO AVAM	OAuth2 Client Cred.	Stellensuchende, Vermittlungsdaten, RAV-Schnittstelle
BGSA-Register	SECO BGSA	Bearer-Token	Meldung bestaetigter Schwarzarbeits-Verstoesse
SAP HCM Finanzbuchhaltung	intern SG	Basic Auth (OData)	Kantonale Finanzbuchhaltung fuer Sanktionsbuchungen
Betreibungsamt SG eSchKG	SG Betreibungsamt	eSchKG Bearer	Uebermittlung von Betreibungsbegehren aus Sanktionen

Im Demo-Modus laufen alle Schnittstellen mit Mock-Antworten. In Produktion werden die echten Bundes- bzw. Kantons-Endpoints konfiguriert.

7 Architektur

Next.js 14 Standalone - PostgreSQL 15 Managed - AWS S3 Object-Storage - Prisma ORM mit Audit-Extension - mandantenfaehig (Tenant SG + SH konfiguriert). Die aktuelle Umgebung dient Demo/Evaluation. Produktive Hosting-Region gemaess Vertrag.

8 HERMES-Dokumente

17 DOKS

Alle Dokumente sind auf der Demo-Umgebung abrufbar (PDF, Zugang auf Anfrage). Markdown-Quellen liegen im Repository unter `/hermes/`.

01 Projektantrag
Projekt-Steckbrief, Zielsetzung, Abgrenzung

02 Studie
Stakeholder-Analyse, Variantenstudie

03 Konzept
Fach-Konzept inkl. State-Machine

04 Anforderungen
Pflichtenheft / 27 Anforderungen

05 ISDS-Konzept
Informationssicherheit + Datenschutz

06 Architektur
Technische Architektur

07 Testkonzept
Teststrategie, Testarten, Akzeptanz

08 Migrationskonzept
Rollout-Plan, Datenmigration

09 Betriebshandbuch
Operations Runbook

10 Testreport
Test-Resultate (UAT, Regression)

11 Lasttest
Skalierungsnachweis, Performance

12 Security-Audit
OWASP Top 10 + ASVS Level 1

13 DSFA
Datenschutz-Folgenabschaetzung

14 Demo-Script
Skript fuer Live-Praesentation

15 Betriebsmodell
Service-Vertrag-Skizze, SLA

16 Referenzprojekte
Anbieter-Referenzen

17 Region-Migration
`us-west-2` -> `eu-central-2`

9 Kontakt und naechste Schritte

Demo-Umgebung und Dokumente

Fuer Fachfragen oder eine Demo-Praesentation bitte direkt an die Projektleitung AWA wenden.

Tour-Seite (ohne Login) und HERMES-Dokumente sind auf der Demo-Umgebung verfuegbar. Zugang auf Anfrage.

Technisch freigegeben fuer Demo/Evaluation. Produktive Aktivierung erfolgt nach kundenseitiger Konfiguration, Schnittstellenabnahme und vertraglicher Freigabe.