DOKUMENTATION & REVISIONSLEITFADEN

GAMPERLAB™ Customer Console — Offizielles Benutzerhandbuch

Vollständige Betriebsdokumentation für die GAMPERLAB™ Customer Console. Dieses Dokument beschreibt die hardware-gestützte Authentifizierung über kryptografische WebAuthn-Passkeys, Flotten- und Schlüsselverwaltung, DORA Art. 12 & § 38 BWG Sanction Sieve™ Compliance, Zero-Downtime Key-Rotation und den regulatorischen 4-Augen GoAML-Meldeprozess für Compliance-Officers und IT-Auditoren.

Version: 2026.10-RELEASE **Stand:** 06. Oktober 2026

Klassifizierung: Öffentlich / Instituts-Standard

Regulierung: DORA Art. 12/13 & § 38 BWG Audit-konform

Inhaltsübersicht

01. Architektur & WebAuthn-Gerätebindung
02. Zero-Trust Authentifizierung & Zugangsverfahren
03. API-Key Management & Zero-Downtime Rotation
04. Flottenverwaltung & Magic Links
05. Sanction Sieve™ DORA & § 38 BWG Cockpit
06. Ad-Hoc Compliance Desk & 4-Augen GoAML
07. Technischer Support & SLA-Garantien

KAPITEL 01

Architektur & WebAuthn-Gerätebindung

Dieses Handbuch beschreibt die GAMPERLAB™ Customer Console: Anmeldung, Kontingente, API-Schlüssel, Geräteregister und die Compliance-Engine für Sanktions- und PEP-Prüfung.

> ⚡ **Kryptografische Gerätebindung:** Die Anmeldung an der GAMPERLAB™ Konsole erfolgt über standardisierte W3C WebAuthn-Passkeys (FIDO2 / Secure Enclave). Es findet keine spekulative Halbleitermessung statt. Die Gerätebindung verankert kryptografische ECDSA P-256 / Ed25519 Schlüsselpaare direkt im Authenticator des Endgeräts.

Die 3 Säulen der Portal-Architektur:

- **Gerätebindung über WebAuthn-Passkeys:** Die Anmeldung erfolgt über einen gerätegebundenen privaten Schlüssel, der den physischen Sicherheitschip (Secure Enclave / TPM) nicht verlassen kann. Der geheime Teil ist nicht auslesbar; serverseitig wird ausschließlich der registrierte öffentliche Schlüssel geprüft.
- **Strikte Mandanten-Isolation:** Jeder API-Key ist über SHA-256 Hashes streng an seinen Mandanten gebunden. Es gibt keine geteilten Status- oder Session-Objekte zwischen verschiedenen Kunden.
- **Souveräne europäische Datenhaltung:** Keine US-Cloud-Abhängigkeiten (US Cloud Act unanwendbar). Die Compliance-Engine arbeitet in-memory im eigenen österreichischen Rechenzentrum (VIX Wien).

KAPITEL 02

Zero-Trust Authentifizierung & Zugangsverfahren

Der Zugang zur GAMPERLAB™ Customer Console ist mehrstufig gesichert, um unautorisierte Zugriffe selbst bei kompromittierten Passwörtern vollständig auszuschließen.

METHODE	SICHERHEITSSTUFE	ABLAUF & VERWENDUNGSZWECK
Hardware-Passkey (WebAuthn)	**Höchste (EAL6+ hardware-gestützt)**	Klick auf *„Mit Hardware-Passkey entsperren“*. Authentifizierung via Touch ID, Face ID oder Windows Hello. Der private Schlüssel verlässt niemals den physischen Sicherheitschip.
API-Key Direkt-Login	**Standard**	Eingabe des im Onboarding erhaltenen Schlüssels (`sieve_live_...` oder `sieve_test_...`). Das System verifiziert den Hash in Echtzeit via Stripe Customer Search.
130-Bit Notfallschlüssel	**Notfall-Recovery**	Wiederherstellung bei Verlust aller Hardware-Geräte mittels GLAB–XXXXX–XXXXX–`...`. Widerruft sofort alle alten Geräte und schützt vor Account-Übernahme.

KAPITEL 03

API-Key Management & Zero-Downtime Key Rotation

In der Sektion **API-Schlüssel Verwaltung** haben Administratoren die vollständige Kontrolle über aktive Produktionsschlüssel.

> ⚠️ **Regelmäßige Rotation empfohlen:** Gemäß PCI-DSS und DORA Art. 9 sollten API-Keys für kritische Zahlungsinfrastrukturen mindestens alle 90 Tage oder bei Mitarbeiterwechseln rotiert werden.

Schritt-für-Schritt: Schlüssel erneuern (Key Rotate)

1. Klicken Sie in der Konsole auf den Button **„Key erneuern (Rotate) ↻“**.
2. Bestätigen Sie die Sicherheitswarnung im Bestätigungsdialog.
3. Das System generiert atomar einen neuen kryptografischen Schlüssel (`sieve_live_...`) und aktualisiert die Autorisierungshashes.
4. Der neue Schlüssel wird **genau einmalig im Klartext angezeigt**. Kopieren und sichern Sie ihn sofort in Ihrem Secret Manager (z.B. HashiCorp Vault oder AWS Secrets Manager).
5. Ihre Portal-Sitzung wird unterbrechungsfrei auf den neuen Schlüssel migriert. Der alte Schlüssel verfällt sofort.

KAPITEL 04

Autorisierte Hardware-Flotte & Magic Links

In der Sektion **Autorisierte Hardware-Flotte** verwalten Sie die physischen Arbeitsstationen und Mobilgeräte, die Zugriff auf Ihre Konsole besitzen.

Neues Gerät koppeln (Scanner-resistenter Magic Link)

Um ein neues Gerät (z.B. Firmen-Laptop oder Management-Tablet) hinzuzufügen:

1. Klicken Sie auf **„+ Weiteres Gerät per Magic Link hinzufügen“**.
2. Geben Sie Ihre autorisierte Firmen-E-Mail-Adresse ein.
3. Sie erhalten eine E-Mail mit einem Einmal-Link, der streng auf 10 Minuten begrenzt und gegen automatisierte E-Mail-Virenscanner gehärtet ist.
4. Öffnen Sie den Link auf dem Zielgerät und berühren Sie den biometrischen Sensor (Touch ID / Face ID / Windows Hello). Das Gerät ist dauerhaft verankert.

1-Klick Hardware Kill-Switch

Bei Verlust oder Außerdienststellung eines Geräts klicken Sie in der Flottentabelle neben dem betroffenen Gerät auf **„Widerrufen ✕“**. Der öffentliche Registrierungsschlüssel wird sofort widerrufen und der Zugang von diesem Gerät dauerhaft gesperrt.

KAPITEL 05

Sanction Sieve™ DORA & § 38 BWG Compliance Cockpit

Das Tab **Sanction Sieve™ Compliance** bietet ein vollständiges Aufsichtscockpit für Banken, Acquirer und Kassennetzbetreiber (ECR).

KENNZAHL / FEATURE	SPEZIFIKATION	BEDEUTUNG FÜR DIE REVISION
Screening Latenz (P99)	**< 0,28 ms**	Echtzeitprüfung im POS/ECR-Autorisierungspfad ohne spürbare Kassenverzögerung.
Sanktionslisten-Umfang	**969.253 Einträge**	EU CFSP, UK OFSI/HMT, US OFAC SDN, UN Resolutionen, SECO Schweiz und PEP-Register.
WORM Audit Ledger	**Ed25519 & Merkle Root**	Revisionssichere Unveränderbarkeit jeder Transaktionsentscheidung gem. DORA Art. 12.
Auto-SAR Engine	**GoAML XML Export**	Automatische Erstellung von Verdachtsmeldungen mit SHAP-Erklärbarkeitsmatrix (EU AI Act Art. 14).

KAPITEL 06

Ad-Hoc Compliance Desk & 4-Augen GoAML Workflow

Der **Ad-Hoc Compliance Desk** ist ein gesicherter Arbeitsplatz für Geldwäschebeauftragte (AML Officers) zur manuellen Einzelfallprüfung von verdächtigen Personen, Unternehmen oder Transaktionen. Um die Kundenkonsole übersichtlich zu halten, ist der Desk autorisierten Compliance-Beauftragten vorbehalten (Aktivierung via Rollen-Berechtigung oder Direktparameter ? `tab=manual`).

> ⚡ **Souveräne In-Memory Anbindung (VIX Wien, AS197540):** Der Desk führt keine Simulationen durch, sondern ist direkt an die Hochleistungs-Engine angebunden. Jede Abfrage prüft über 960.000 tagesaktuelle Einträge (OFAC SDN, EU CFSP, UK FCDO, UN, SECO) in unter 0,20 ms und erzeugt ein revisionssicheres SHA-256 WORM-Protokoll gem. DORA Art. 12 und § 38 BWG.

Der regulatorische 4-Augen-Freigabeprozess:

1. Wird eine Übereinstimmung mit einer Sanktions- oder PEP-Liste erkannt, wechselt die Transaktion in den Status `ESCROW (4-AUGEN)`.
2. Ein zweiter autorisierter Compliance-Officer prüft die Trefferquote, SHAP-Explainability-Werte und Treffergründe im Dossier.
3. Mit einem Klick auf **„✓ 4-Augen Freigeben“** wird die Freigabe kryptografisch mit Officer-ID und Zeitstempel signiert.
4. Über den Button **„📩 GoAML-XML“** wird die offizielle Verdachtsmeldung im standardisierten XML-Format für die Financial Intelligence Unit (FIU) exportiert.

KAPITEL 07

Technisches Support Desk & SLA-Garantien

In der Sektion **Technischer Support & Incident Desk** können autorisierte Kunden verifizierte Support-Tickets eröffnen.

> 📋 **Strukturierte Fehler-Telemetrie:** Bei Eröffnung eines Tickets werden technische Metadaten (Plattform-Umgebung, WebCrypto-Verfügbarkeit, mTLS-Verbindungsstatus) strukturiert und datenschutzkonform an das Incident Desk übermittelt.

Garantierte Service Level Agreements (SLA):

- **Enterprise Tier:** 2 Stunden Notfall-SLA (24/7 Notfall-Eskalation mit direktem Lead Architect Dispatch).
- **Growth Tier:** 24 Stunden Reaktionszeit an Werktagen für Schnittstellen- und Abrechnungssupport.
- **Developer Tier / Sandbox:** 48 Stunden Entwickler-Support (Best-Effort) für API-Integration.

© 2026 GAMPERLAB™ — Financial Compliance & Infrastructure Laboratory. Kufstein (Austria). Alle Rechte vorbehalten.