CashRadar — Security & Datenschutz (Überblick)

Produkt: CashRadar — SaaS-Plattform für Cash-at-Risk & Forderungsmanagement **Anbieter:** Tridico Beteiligungen UG (haftungsbeschränkt), Deutschland **Hosting (Datenbank/Storage):** Supabase auf **AWS Stockholm, EU (eu-north-1) Stand:** 2026-06-03 · **Kontakt:** hello@cashradar.io **Reifegrad:** Pilot-/Frühphase — DSGVO-Architektur umgesetzt; finale juristische Abnahme vor Produktivbetrieb.

> *Dieses Dokument beschreibt ausschließlich verifizierte Maßnahmen. Aussagen, die nicht belegt werden konnten, wurden bewusst weggelassen.*

Kernzusagen

- ■ EU-Hosting (Stockholm, eu-north-1) für Datenbank, Auth, Storage
- ■ Strikte Mandantentrennung über Row-Level Security (RLS)
- ■ Verschlüsselung: TLS 1.2+ im Transport, AES-256 im Ruhezustand
- ■ Append-only Audit-Log kritischer Aktionen
- ■ Rollenbasierte Zugriffskontrolle (RBAC)
- ■ Schutz gegen geleakte Passwörter (HaveIBeenPwned) aktiviert
- ■ Daten-Export & Löschung jederzeit

1. Architektur & Datenresidenz

Cloud-native Multi-Tenant-SaaS. Die **Forderungs-/Debitoren-Kerndaten** werden ausschließlich in der EU verarbeitet und gespeichert.

Komponente	Anbieter	Standort	Schutzmaßnahmen
Datenbank, Auth, Storage	Supabase (auf AWS)	**Stockholm, EU (eu-north-1)**	RLS, AES-256 at rest, tägliche Backups
Frontend-Hosting	**Lovable**	*(Region: zu bestätigen)*	TLS, statisches Frontend (Mandantendaten laufen Browser↔Supabase)
Transaktionale E-Mails	Resend	**EU (eu-west-1, Irland)** — Domain cashradar.io	TLS, SPF/DKIM/DMARC
Fehler-Monitoring	Sentry	**EU-Region** (Org: Tridico Beteiligungen UG)	PII-Scrubbing

> ***Datenstandort: vollständig EU.*** *Datenbank/Storage (Supabase, Stockholm), Fehler-Monitoring (Sentry, EU) und E-Mail-Versand (Resend, Irland/eu-west-1, Domain cashradar.io) verarbeiten ausschließlich in der EU. CashRadar setzt* ***keine KI*** *ein → **kein Drittlandtransfer personenbezogener Daten**. (Das statische Frontend wird über Lovable ausgeliefert; Mandantendaten laufen dabei direkt Browser↔Supabase, nicht über Lovable.)*

2. Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Mandantentrennung:** Row-Level Security auf **allen 28 Tabellen** (99 Policies, davon 6 mit FORCE RLS). Jede Policy filtert über `organization_id` (Funktion `get_user_organization`/`has_role`).
- **RBAC:** Rollen admin / member / viewer in separater `user_roles`-Tabelle (keine Rechte- Eskalation über Profil-Manipulation).
- **Authentifizierung:** Supabase Auth, bcrypt-Passwort-Hashing, JWT-Sessions mit Auto-Refresh, **Leaked-Password-Schutz (HIBP) aktiviert.**
- **Secrets:** Service-Role-Schlüssel ausschließlich serverseitig (nie im Client).

Integrität

- **Audit-Log:** append-only (kein UPDATE/DELETE), protokolliert Status-, Klärfall-, Mahn- und PTP-Änderungen mit Benutzer-ID und Zeitstempel; Soft-Delete für Timeline-Einträge.
- **DB-Trigger:** erzwingen `created_by`, setzen `deleted_by` bei Soft-Delete, validieren Belegarten.
- **Beträge** als `NUMERIC` (kein Floating-Point) → keine Rundungsfehler.
- **Edge Functions:** JWT-/Rollenprüfung; privilegierte Operationen mit HMAC-Signatur + Replay-Schutz.

Verfügbarkeit

- Managed-Infrastruktur (Supabase/AWS, EU). **Tägliche automatische Backups.**
- *(Point-in-Time-Recovery derzeit nicht aktiviert; keine Multi-AZ-/Failover-Zusage; Verfügbarkeit Best-Effort.)*

Überprüfung

- Automatisierte Sicherheits-Tests (RLS/Cross-Org/Rollen/Unauth) vor Releases.
- Kontinuierliche Security-Scans der Codebase.

3. Unterauftragsverarbeiter (Sub-Prozessoren)

Anbieter	Zweck	Standort	Status
Supabase	Datenbank, Auth, Storage	EU / Stockholm (eu-north-1)	**DPA abgeschlossen (04.06.2026, EU-SCC)**
Lovable	Frontend-Hosting / Deployment	*(Region zu bestätigen)*	**DPA abgeschlossen (24.11.2025, EU-SCC)**
Resend (Resend Inc., US)	Transaktionale E-Mails	Verarbeitung EU (eu-west-1, Irland)	**DPA inkl. EU-SCC**
Sentry	Fehler-Monitoring (PII-gescrubbt)	**EU-Region**	**DPA abgeschlossen (04.06.2026, EU-SCC)**

> ***Alle vier Sub-Prozessor-DPAs abgeschlossen*** *(Supabase, Resend, Lovable, Sentry — jeweils mit EU-SCC).*
> ***Keine KI:*** *CashRadar setzt* ***keine KI*** *ein. Es gibt keinen KI-/LLM-Sub-Prozessor; es werden* ***keine*** *Daten an Google (Gemini) oder andere KI-/LLM-Dienste übermittelt. Alle Auswertungen (inkl. Spaltenerkennung beim Import) erfolgen ausschließlich regelbasiert.*

4. Datenkategorien, Speicherung, Betroffenenrechte

- **Datenkategorien:** Debitoren-Stammdaten; Kontaktpersonen (Name, E-Mail, Telefon); Forderungs- daten (Beträge, Fälligkeiten, Status); Nutzerdaten; Aktivitäts-/Audit-Daten. **Keine** besonderen Kategorien nach Art. 9 DSGVO.
- **Speicherung:** während der Vertragslaufzeit; Löschung nach Vertragsende.
- **Betroffenenrechte:** Daten-Export und Löschfunktionen in der Plattform; Auskunfts-Ersuchen werden an den Verantwortlichen weitergeleitet.

5. Incident Response

Sofortmaßnahmen (Secret-Rotation, Session-Invalidierung, Audit-Log-Export), Umfangsbestimmung, Unterstützung des Kunden bei Meldungen nach Art. 33/34 DSGVO (72 h).

6. Compliance-Posture (ehrlich)

Punkt	Status
EU-Datenresidenz (Kerndaten)	■ Stockholm (eu-north-1)
Verschlüsselung at rest / in transit	■ AES-256 / TLS 1.2+
Mandantentrennung (RLS)	■ 28 Tabellen / 99 Policies
Leaked-Password-Schutz	■ aktiviert
Eigene Zertifizierungen (ISO 27001 / SOC 2)	■ nicht vorhanden (Frühphase)
Infrastruktur-Zertifizierungen Sub-Prozessoren	AWS ISO 27001, Supabase SOC 2 Type II
DSGVO-Konformität	**DSGVO-Architektur (Pilot)** — finale juristische Abnahme ausstehend

Betrieb: Anbieter ist die Tridico Beteiligungen UG (haftungsbeschränkt) — eine Kapitalgesellschaft, **kein** Einzelunternehmen; derzeit als Ein-Personen-Gesellschaft betrieben (1 zugriffsberechtigte Person), keine geteilten Accounts.
