Anlage 1 zum Auftragsverarbeitungsvertrag (AVV)

Technische und Organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Auftragnehmer: Tridico Beteiligungen UG (haftungsbeschränkt), Betreiber von CashRadar **Stand:** 2026-06-04 · **Version:** 3.1 (faktengeprüft, alle Aussagen verifiziert) **Kontakt:** hello@cashradar.io

> *Diese Anlage enthält ausschließlich verifizierte Maßnahmen. Aussagen, die nicht belegt werden konnten (z. B. Zertifizierungen, größere Infrastruktur-Tiers), wurden entfernt.*

---

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b)

1.1 Zutrittskontrolle (physisch)

Es wird keine eigene Server-Infrastruktur betrieben. Die Verarbeitung erfolgt in den zertifizierten Rechenzentren der Sub-Auftragsverarbeiter (Supabase auf **AWS, Region Stockholm / eu-north-1**). Physische Sicherheit (Zutritts-/Videokontrolle, ISO-27001-zertifizierte RZ) wird durch AWS gewährleistet; Mitarbeiter des Auftragnehmers haben keinen physischen Serverzugang.

1.2 Zugangskontrolle (Systemzugang)

- Authentifizierung über **Supabase Auth** mit bcrypt-Passwort-Hashing, JWT-Sessions mit Auto-Refresh.
- **Schutz gegen geleakte Passwörter (HaveIBeenPwned / Leaked Password Protection): aktiviert.**
- Rate-Limiting der Authentifizierungs-Endpunkte (Supabase-seitig).
- Individuelle Konten, keine geteilten Accounts.

1.3 Zugriffskontrolle (Datenzugriff)

- **Row-Level Security (RLS) auf allen 28 Datenbank-Tabellen** (insgesamt 99 Policies, davon 6 Tabellen mit FORCE RLS).
- Mandantentrennung über `organization_id` in jeder Policy (Funktionen `get_user_organization`, `has_role`). *(Eine feinere Trennung nach Entitäten innerhalb einer Organisation erfolgt auf Anwendungsebene, nicht auf RLS-Ebene.)*
- Rollenmodell (RBAC): admin / member / viewer in separater `user_roles`-Tabelle; privilegierte Operationen (Audit-Log, Org-Settings) admin-only.
- Service-Role-Schlüssel ausschließlich in Edge Functions (serverseitig), niemals im Client.

1.4 Trennungskontrolle

- Logische Mandantentrennung über RLS auf jeder Zeile.
- Demo-/Test-Mandanten existieren als eigene Organisationen und sind über dieselbe RLS-Mandantentrennung von Produktivdaten getrennt.

1.5 Pseudonymisierung

- Audit-Logs verwenden User-IDs (UUIDs) statt Klarnamen.
- Telemetrie-/Usage-Events enthalten keine personenbezogenen Daten (nur Aktions-Typen + IDs).
- Fehler-Monitoring (Sentry) mit PII-Scrubbing in Stack-Traces (E-Mails, IDs, Namen maskiert).

2. Integrität (Art. 32 Abs. 1 lit. b)

2.1 Weitergabekontrolle (Transport)

- **TLS 1.2+** für sämtliche Verbindungen.
- E-Mail-Versand über Resend (Resend Inc., US-Gesellschaft; Verarbeitung in der **EU-Region, eu-west-1/Irland**, abgedeckt durch EU-SCC), Domain **cashradar.io**, mit SPF/DKIM/DMARC. Versand ausschließlich von `noreply@cashradar.io`.
- Keine Übertragung über unverschlüsselte Kanäle.
- Datei-Downloads nur für authentifizierte Nutzer.

2.2 Eingabekontrolle

- Append-only `audit_log`: Wer hat wann welches Objekt verändert.
- Vollständige Ereignis-Historie pro Rechnung (Status, Owner, Disputes, Notizen, Kontakte).
- `created_by`/`updated_by`-Felder; Audit-Log nicht durch Nutzer änder-/löschbar.
- Status-Änderungen (z. B. PTP) werden per DB-Trigger protokolliert.

2.3 Datenintegrität

- Validierung auf DB-Ebene über Constraints und Trigger (z. B. `validate_invoice_type`).
- TypeScript-Typen aus dem DB-Schema generiert.
- Idempotente Importe mit Duplikat-Erkennung anhand Rechnungsnummer.
- Geldbeträge als `NUMERIC` (kein Floating-Point).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b)

3.1 Backup

- **Tägliche automatische Backups** (Supabase Managed Backups, in der EU-Region).
- Backups verschlüsselt (AES-256 at rest).
- **Point-in-Time-Recovery ist derzeit nicht aktiviert.** Daraus folgt ein maximaler Wiederherstellungspunkt (RPO) von bis zu 24 Stunden (letztes Tages-Backup).

3.2 Verfügbarkeit / Resilienz

- Managed, serverless-nahe Infrastruktur mit automatischer Skalierung der Edge Functions.
- Verfügbarkeit auf Best-Effort-Basis; keine vertraglich zugesicherte SLA, kein Multi-AZ-/ Automatik-Failover-Setup auf der aktuellen Instanzgröße.

3.3 Notfall-Plan (Incident Response)

Phase	Maßnahme	Zeitrahmen
Erkennung	Monitoring-Alert / Meldung	zeitnah
Eindämmung	Sperrung kompromittierter Konten, Secret-Rotation, Session-Invalidierung	unverzüglich nach Kenntnis
Information	Information betroffener Verantwortlicher bei Datenschutzvorfällen	ohne unangemessene Verzögerung
Behörden-Meldung (Art. 33)	Unterstützung des Verantwortlichen bei der Meldung	≤ 72 Std.
Wiederherstellung	Restore aus Backup	gemäß Backup-Stand

4. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)

- Wiederherstellung aus täglichen Backups in der EU-Region.
- Backup-Verschlüsselung AES-256 at-rest.

5. Löschkonzept

- **Daten-Export** (JSON) und **Löschfunktionen** in der Plattform vorhanden.
- Bei Vertragsende: Löschung/Rückgabe der personenbezogenen Daten auf Wahl des Verantwortlichen; Löschbestätigung auf Anforderung.
- Betroffenenrechte (Art. 17) werden auf Weisung des Verantwortlichen umgesetzt; bei gesetzlicher Aufbewahrungspflicht erfolgt Sperrung statt Löschung.
- Backups werden gemäß Anbieter-Rotation überschrieben.

6. Auftragskontrolle (Art. 28 DSGVO)

- **Auftragsverarbeitungsverträge mit allen Sub-Auftragsverarbeitern abgeschlossen: Supabase (04.06.2026), Resend, Lovable (24.11.2025) und Sentry (04.06.2026) — jeweils mit EU-Standardvertragsklauseln.**

- **Personenbezogene Daten werden ausschließlich in der EU verarbeitet:** Supabase (EU/Stockholm – eu-north-1), Resend (E-Mail, Domain cashradar.io, EU/eu-west-1 – Irland), Sentry (Fehler- Monitoring, EU-Region, Org Tridico Beteiligungen UG).
- Lovable liefert ausschließlich das **statische Frontend** aus (Deployment); dort werden **keine personenbezogenen Daten gespeichert oder verarbeitet** (Mandantendaten laufen direkt Browser↔Supabase). Die Region des statischen Hostings ist datenschutzrechtlich nicht maßgeblich.
- **CashRadar setzt keine KI ein:** kein KI-/LLM-Sub-Prozessor, kein Datentransfer an Google (Gemini) oder andere KI-/LLM-Dienste. Alle Auswertungen erfolgen regelbasiert.
- **Im Ergebnis: kein Drittlandtransfer personenbezogener Daten.**
- Vorab-Information bei Wechsel/Hinzufügen von Sub-Auftragsverarbeitern; Widerspruchsrecht.

7. Audit- und Überprüfungsverfahren

- **Intern:** automatisierte RLS-/Cross-Org-/Rollen-Sicherheitstests (Test-Suite `e2e/security-rls.spec.ts`) sowie plattformseitige Security-Scans (Lovable).
- **Audit-Recht des Verantwortlichen:** Self-Assessment (Fragebogen) kostenfrei; Remote-Audit (Video-Call mit Dokumentenvorlage) nach Abstimmung.

8. Organisatorische Maßnahmen

- Der Auftragnehmer ist die **Tridico Beteiligungen UG (haftungsbeschränkt)** — eine Kapitalgesellschaft, **kein** Einzelunternehmen. Der Betrieb erfolgt derzeit als **Ein-Personen-Gesellschaft** mit **einer zugriffsberechtigten Person** (Gesellschafter- Geschäftsführer); keine geteilten Accounts.
- Zugriff auf die Anbieter-Konsolen (Supabase/Lovable/Resend) passwortgeschützt.
- Eine externe Datenschutzbeauftragte wird bei Erreichen der gesetzlichen Schwelle benannt.

9. Aktualisierung

Diese TOM werden bei wesentlichen Änderungen (neue Sub-Auftragsverarbeiter, geänderte Verarbeitungszwecke) angepasst und dem Verantwortlichen mitgeteilt.

Tridico Beteiligungen UG (haftungsbeschränkt) · security@cashradar.io · Stand 2026-06-04 · TOM v3.1 (faktengeprüft).