

Technische und organisatorische Maßnahmen (TOM) – Transparify

Version: tom-2026-10-22-f

Technische und organisatorische Maßnahmen (TOM) – Transparify

Stand: 2026-10-22

Diese TOM beschreiben die von Tiemann & Böker UG (haftungsbeschränkt) („Transparify“) getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO für den Betrieb der SaaS-Anwendung Transparify. Sie gelten als Anlage 2 zum Auftragsverarbeitungsvertrag in der jeweils aktuellen Fassung.

Verantwortlich für den Betrieb:

Tiemann & Böker UG (haftungsbeschränkt)

An den Linden 21, 91171 Greding, Deutschland

Amtsgericht Nürnberg, HRB 46477

vertreten durch Nikolai Tiemann

1. Gegenstand und Systemarchitektur

Transparify ist eine Cloud-SaaS zur geführten Ermittlung und Dokumentation wirtschaftlicher Eigentümer. Die Anwendung basiert auf Next.js und wird bei Vercel betrieben. Persistente Geschäftsdaten liegen in PostgreSQL bei Supabase (AWS-Region eu-west-1, Irland); der Zugriff erfolgt serverseitig über Prisma. Die Anmeldung des Hauptprodukts erfolgt über NextAuth (E-Mail/Passwort), optional mit TOTP-Zwei-Faktor-Authentifizierung. Es wird keine Supabase Auth für das Hauptprodukt eingesetzt.

Der primäre Anwendungsbetrieb von Transparify erfolgt in Frankfurt am Main (Vercel). Builds und Edge-/Middleware-Komponenten können multi-regional laufen; eine ausschließlich europäische Verarbeitung aller Komponenten ist nicht gegeben.

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

2.1 Zugangskontrolle

Der Zugang zur Produktionsumgebung und zu sicherheitsrelevanten Zugangsdaten ist auf berechnigte Personen beschränkt. Cloud-Zugangsdaten, API-Schlüssel und andere sicherheitsrelevante Geheimnisse werden über geschützte Umgebungsvariablen und die vorgesehenen Sicherheitsmechanismen der eingesetzten Hosting-Infrastruktur (Vercel) verwaltet.

2.2 Zugriffskontrolle und Mandantentrennung

Alle Mandanten nutzen dieselbe Datenbankinstanz (logische Trennung). Ermittlungen sind dem jeweiligen Benutzerkonto zugeordnet. Zugriffe werden in der Anwendung geprüft (Ownership und, bei Enterprise, Freigaben). Es gibt keine physisch getrennten Datenbanken je Kunde und keine Row-Level-Security als Hauptmechanismus des Produktkerns.

2.3 Authentifizierung

Anmeldung mit E-Mail und Passwort (Passwort-Hash). Optionale Zwei-Faktor-Authentifizierung per TOTP (Authenticator-App). Sitzungen über NextAuth.

2.4 Verschlüsselung

Transport: HTTPS/TLS. Speicherung: Infrastrukturverschlüsselung der Cloud-Anbieter sowie anwendungsseitige Verschlüsselung zentraler Ermittlungs-/Entwurfs-/Watchlist-Felder (AES-256-GCM), soweit im Produkt aktiviert und mit Schlüssel konfiguriert. Nicht alle Felder (z. B. Kontometadaten, Rechnungsreferenzen) sind anwendungsseitig verschlüsselt. Kundenverwaltete Schlüssel (BYOK) werden nicht angeboten.

3. Integrität

Änderungen an Ermittlungsdaten erfolgen über authentifizierte Anwendungsschnittstellen. Concurrent Edits folgen dem Last-Write-Wins-Modell der Anwendung. Wesentliche Betriebsvorgänge (Zahlungen, Zustimmungen) werden über Anbieter-Webhooks bzw. append-only Nachweistabellen nachvollziehbar gehalten.

4. Verfügbarkeit und Belastbarkeit

Hosting und Datenbank nutzen die Verfügbarkeitsmechanismen der Cloud-Anbieter. Die Anwendung wird auf der Serverless-Infrastruktur von Vercel betrieben. Die produktive PostgreSQL-Datenbank wird von Supabase als verwalteter Dienst betrieben. Transparify betreibt keine eigene Multi-AZ-Architektur außerhalb dieser Plattformen.

Supabase erstellt täglich Backups der produktiven PostgreSQL-Datenbank. Die Aufbewahrungsdauer der Backups richtet sich nach dem gebuchten Anbieterplan. Öffentliche Service-Zielwerte (Verfügbarkeit, RPO/RTO) sind Zielwerte ohne Service Credits.

5. Verfahren zur Wiederherstellung

Die Wiederherstellung technischer Systeme erfolgt über die Backup- und Restore-Funktionen der Cloud-Anbieter. Die produktive Datenbank wird aus den täglichen Datenbanksicherungen von Supabase wiederhergestellt. Die Anwendung wird durch erneutes Deployment auf Vercel wiederhergestellt. Es werden keine festen Wiederherstellungsfristen als Vertragsgarantie zugesichert; öffentliche Service-Zielwerte bleiben unverbindliche Zielwerte.

6. Auftragskontrolle und Unterauftragsverarbeiter

Unterauftragsverarbeiter im Sinne von Art. 28 DSGVO für den Betrieb der Anwendung sind insbesondere Vercel (Hosting), Supabase (Datenbank) und Brevo (transaktionaler E-Mail-Versand). Mit den eingesetzten Auftragsverarbeitern bestehen Vereinbarungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO. Weitere Empfänger (z. B. Stripe als Zahlungsdienst, Handelsregister.ai und GeoNames als Datenquellen) sind in der Unterauftragsverarbeiter-/Empfängerliste mit ihrer jeweiligen Rolle beschrieben und nicht pauschal als Unterauftragsverarbeiter der UBO-Akte einzuordnen.

Weisungen des Kunden ergeben sich aus dem Hauptvertrag, dem AVV und der Nutzung der Software.

7. Trennungskontrolle

Produktionsdaten werden von Entwicklungsartefakten getrennt betrieben (produktive Cloud-Umgebung). Test- und Preview-Deployments sind keine vertragliche Kunden-Staging-Umgebung.

8. Eingabekontrolle und Nachvollziehbarkeit

Nutzeraktionen erfolgen nach Anmeldung. Elektronische AVV-Zustimmungen werden append-only mit Unternehmenssnapshot, Dokumentfassung und Zeitpunkt gespeichert. Zahlungsereignisse werden über Stripe-Webhooks verarbeitet.

9. Verfügbarkeitskontrolle und Incident-Management

Sicherheitsvorfälle werden hinsichtlich ihrer Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten bewertet und entsprechend behandelt. Bei Verletzungen des Schutzes personenbezogener Daten informiert Transparify betroffene Auftraggeber gemäß Art. 33 Abs. 2 DSGVO unverzüglich nach Bekanntwerden des Vorfalls. Die Meldung an die zuständige Aufsichtsbehörde obliegt dem jeweiligen Verantwortlichen, soweit Transparify ausschließlich als Auftragsverarbeiter tätig ist.

10. Datenschutz durch Technikgestaltung

Datensparsamkeit: Es werden nur für Ermittlung, Konto, Abrechnung und Betrieb erforderliche Daten erhoben. Öffentliche Registerdaten werden serverseitig abgerufen. Keine produktive KI-Dokumentenanalyse im Standardangebot. Kein Dokumentenmanagementsystem.

11. Überprüfung und Anpassung

Transparify darf Maßnahmen an den Stand der Technik anpassen, sofern das Schutzniveau nicht sinkt. Wesentliche Änderungen werden dokumentiert. Prüfberichte und Zertifikate der Infrastrukturanbieter (soweit vom Anbieter veröffentlicht) können als Nachweise der Unterauftragsverarbeiter herangezogen werden; sie gelten nicht als eigene ISO-27001- oder SOC-2-Zertifizierung von Transparify.

12. Bezugsdokumente

- Auftragsverarbeitungsvertrag: /legal/dpa
- Empfänger- und Unterauftragsverarbeiterliste: /legal/subprocessors
- Service-Zielwerte: /legal/service-levels