Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO)

Version 2.0 · Produkt: DigitalTwin Plattform · Organisation: Ankerkern, Warthestr. 48, 12051 Berlin · Stand: Juni 2026

1. Ziel und Schutzbedarf

Diese Maßnahmen schützen personenbezogene Daten, die durch die DigitalTwin-Architektur verarbeitet werden, gemäß Art. 32 DSGVO. Der Schutzbedarf ist als „normal bis hoch“ eingestuft. Ein hoher Schutzbedarf gilt insbesondere für:

- Kommunikationsinhalte (E-Mail, Sprache, Dokumente und Freitexte),
- Finanz-, Buchhaltungs-, Projekt-, Bestands-, Waren- und Fuhrparkdaten in Workflows und ERP-Prozessen,
- Mandanten-Secrets, API-Schlüssel, OAuth-Token und Webhook-Secrets.

Hinweis: Die systematische Verarbeitung von Gehalts- und Lohnabrechnungsdaten oder besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) ist technisch eingeschränkt und vertraglich ausgeschlossen.

2. Pseudonymisierung und Verschlüsselung

Bereich	Maßnahme
Verschlüsselung ruhender Daten	Alle Datenbanken und persistenten Container-Volumes sind vollständig at rest verschlüsselt. Die Verschlüsselung wird auf Volume-Ebene (LUKS/dm-crypt) über den Infrastrukturanbieter (IONOS) mit AES-256 erzwungen.
Verschlüsselung bei Übertragung	Ende-zu-Ende-TLS-1.2+-Verschlüsselung für sämtlichen Web-/API-/Auth-Verkehr über Caddy Reverse Proxy. SMTP- und OAuth-Verkehr strikt über TLS. WebRTC/SIP/RTP nach Protokollstandards abgesichert.
Secret-Management	Mandanten-Secrets werden AES-256-GCM-verschlüsselt in der Datenbank gespeichert (per Master Key). Infrastruktur- und Deployment-Secrets werden ausschließlich zur Laufzeit über GitHub Secrets/Infisical injiziert.

3. Mandantentrennung und Isolation

Die Architektur erzwingt strikte logische und Container-basierte Grenzen, um mandantenübergreifende Datenabflüsse zu verhindern:

- **Datenbank-Isolation:** Striktes Schema-pro-Mandant-Prinzip auf Datenbankebene. Backend-Filter erzwingen die Kontext-Extraktion aus validierten JWT-Claims.
- **Speicher-Isolation:** Dedizierte S3-Buckets je Mandant für Dokumente und Assets.
- **Workflow-Isolation:** Dedizierte Container-Instanzen je Mandant. Agenten arbeiten in strikt isolierten Mandanten-Kontexten.
- **Authentifizierung:** Strikte rollenbasierte Zugriffskontrolle (RBAC). Trennung der Rollen Plattform-Admin, Mandanten-Admin und Mandanten-Nutzer.

4. Zugriffskontrolle (Vertraulichkeit)

- **Administrativer Zugriff:** Der administrative Zugriff auf Produktionsdatenbanken und Infrastruktur ist technisch auf maximal 3 autorisierte Personen beschränkt. Alle administrativen Aktionen erfordern Multi-Faktor-Authentifizierung (MFA) über IONOS, GitHub und die Token-Management-Plattform und werden unveränderlich protokolliert.

- **Anwendungszugriff:** Nutzerzugriff erfordert starke Passwort-Richtlinien (gehashte Speicherung). MFA-Integrationen werden über Microsoft EntraID oder Google Workspace unterstützt.

5. KI-, Prompt- und Agenten-Schutzmaßnahmen

Aufgrund der Integration von LLMs (OpenAI, Anthropic, Google, IONOS OS) werden spezifische Leitplanken durchgesetzt:

- **Zero-Training-Policy:** Vertragliche Garantien stellen sicher, dass keine Kundendaten, Prompts oder Transkripte zum Training von Foundation-Modellen genutzt werden.
- **Prompt-Templates vs. Sessions:** Prompt-Templates stellen proprietäre Systemlogik dar und werden unbefristet vorgehalten. Prompt-Sessions (mit potenziellen ERP-/Kommunikationsdaten des Kunden) werden für 24 Monate zur Sicherung einer prüffähigen Geschäftshistorie gespeichert und anschließend systematisch gelöscht.

6. Verfügbarkeit und Belastbarkeit

Hohe Verfügbarkeit wird über automatisierte Deployments (Terraform/Docker Compose) und durchgängige CI/CD-Pipelines mit verpflichtenden E2E-Tests vor jedem Merge auf den Main-Branch sichergestellt.

- **Backup-Strategie:** Tägliche inkrementelle Backups mit 7 Tagen Vorhaltung; wöchentliche Voll-Backups mit 12 Wochen Vorhaltung.
- Backups sind verschlüsselt und werden in verwalteten, vom Laufzeitbetrieb getrennten S3-Buckets bei IONOS gespeichert, logisch je Mandant getrennt.
- Disaster-Recovery-Übungen und Wiederherstellungsprozesse werden jährlich getestet und dokumentiert.

7. Regelmäßige Überprüfung

Die Wirksamkeit der Maßnahmen wird regelmäßig überprüft und an den Stand der Technik angepasst; wesentliche Änderungen werden dokumentiert. Dieses Dokument ist Bestandteil der Anlage 3 des Auftragsverarbeitungsvertrags (AVV) von Ankerkern.

Nur die deutsche Fassung dieses Dokuments ist rechtlich maßgeblich. Die englische Übersetzung dient ausschließlich Informationszwecken.

ENGLISH VERSION

Non-binding translation · Only the German version is legally authoritative

ankerkern

TRUST & COMPLIANCE

Technical and Organizational Measures (TOMs)

pursuant to Art. 32 General Data Protection Regulation (GDPR)

Version 2.0 · Product: DigitalTwin Platform · Organization: Ankerkern, Warthestr. 48, 12051 Berlin · As of: June 2026

1. Objective and Protection Requirements

These measures safeguard personal data processed by the DigitalTwin architecture in accordance with Article 32 GDPR. The protection requirement is categorized as normal to high. High protection applies specifically to:

- communication content (email, voice, documents, and free text),
- finance, accounting, project, inventory, goods, and fleet data utilized in workflows and ERP processes,
- tenant secrets, API keys, OAuth tokens, and webhook secrets.

Note: The systematic processing of payroll data or special categories of data (Article 9 GDPR) is technically restricted and contractually excluded.

2. Pseudonymization and Encryption

Domain	Measure
Encryption at rest	All databases and persistent container volumes are fully encrypted at rest. Encryption is enforced at the volume level (LUKS/dm-crypt) via the infrastructure provider (IONOS) utilizing AES-256.
Encryption in transit	End-to-end TLS 1.2+ encryption for all web/API/auth traffic via Caddy reverse proxy. SMTP and OAuth traffic strictly routed over TLS. WebRTC/SIP/RTP secured according to protocol standards.
Secret management	Tenant secrets are AES-256-GCM encrypted within the database (via master key). Infrastructure and deployment secrets are injected strictly at runtime via GitHub Secrets/Infisical.

3. Tenant Separation and Isolation

The architecture enforces rigorous logical and container-level boundaries to prevent cross-tenant data leakage:

- **Database isolation:** Strict schema-per-tenant architecture on database level. Backend filters enforce context extraction from validated JWT claims.
- **Storage isolation:** Dedicated S3 buckets for each client's documents and assets.
- **Workflow isolation:** Dedicated container instances allocated per tenant. Agents operate in strictly isolated tenant contexts.
- **Authentication:** Strict role-based access control (RBAC). Separation of platform-admin, tenant-admin, and tenant-user roles.

4. Access Control (Confidentiality)

- **Administrative access:** Administrative access to production databases and infrastructure is technically restricted to a maximum of 3 authorized personnel. All administrative actions require multi-factor authentication (MFA) across IONOS, GitHub, and the token management platform, and are logged immutably.

- **Application access:** User access requires strong password policies (hashed storage). MFA integrations are supported via Microsoft EntraID or Google Workspace.

5. AI, Prompt, and Agent Safeguards

Due to the integration of LLMs (OpenAI, Anthropic, Google, IONOS OS), specific guardrails are enforced:

- **Zero-training policy:** Contractual guarantees enforce that no customer data, prompts, or transcriptions are utilized for training foundational LLM models.
- **Prompt templates vs. sessions:** Prompt templates represent proprietary system logic and are retained indefinitely. Prompt sessions (containing potential client ERP/communication data) are retained for 24 months to maintain an auditable business history, after which they are systematically deleted.

6. Availability and Resilience

High availability is maintained via automated deployments (Terraform/Docker Compose) and comprehensive CI/CD pipelines enforcing E2E testing prior to merging to the main branch.

- **Backup strategy:** Daily incremental backups retained for 7 days; weekly full backups retained for 12 weeks.
- Backups are encrypted and stored in managed, off-runtime S3 buckets at IONOS, logically separated by tenant.
- Disaster recovery drills and restore processes are tested and documented annually.

7. Regular Review

The effectiveness of the measures is reviewed regularly and adapted to the state of the art; material changes are documented. This document forms part of Annex 3 of the Ankerkern Data Processing Agreement (DPA).

Only the German version of this document is legally authoritative. The English translation is provided for information purposes only.