AUDIT-08 — Scope

Stand: 2026-05-18

In-Scope

Verarbeitungstätigkeiten

1. **Mandanten-Onboarding** — Koordinator-Kontaktdaten + Koordinator-Geschäftsanschrift; AVV-Abschluss
2. **Vorgangs-Bearbeitung** — Hersteller-Stammdaten + technische Unterlagen, OPL-Klärungs-Mails, Akten-Versionen
3. **Koordinator-Workspace-Hosting** — Mandanten-Verzeichnis mit allen Vorgangs-Artefakten
4. **Mail-Bridge** — IMAP-Eingang + SMTP-Versand für Hersteller-Kommunikation
5. **Sub-Verarbeiter-Aufrufe** — LLM-Calls an Mistral/Anthropic mit Hersteller-Stammdaten als Prompt-Kontext
6. **Backup + 10-Jahres-Archiv** — Akten-Snapshots + Koordinator-Kontaktketten

Datenkategorien

Kategorie	Beispiel	Schutzklasse
Koordinator-Identifikation	Name, Geschäftsanschrift, Berufshaftpflicht-Nummer	normal
Hersteller-Identifikation	Firmenname, USt-ID, Geschäftsführer	normal
Technische Unterlagen	Stücklisten, Schaltpläne, Risiko-Bewertungen	erhöht (Betriebsgeheimnis)
Kommunikations-Daten	E-Mail-Adressen Hersteller-Mitarbeiter, Mail-Text	normal
OPL-Antworten	Hersteller-Antworten zu Klärungs-Fragen	erhöht
Telemetrie	Pipeline-Logs, OPL-Statistiken (anonymisiert)	normal

Keine Art-9-Sonderkategorien (Gesundheit, biometrisch, politisch etc.) werden systematisch verarbeitet. Wenn ein technisches Dokument zufällig PII enthält (z. B. Konstrukteurs-Namen in CAD-Headern), ist das tenant-intern und verlässt unsere Infrastruktur nur an die vertraglich gebundenen Sub-Verarbeiter.

Betroffene Personen

1. Koordinator-Mitarbeiter (i. d. R. der Koordinator selbst, eine Person)
2. Hersteller-Mitarbeiter (Geschäftsführer, Konstrukteure, Sicherheitsingenieure)
3. Endkunden des Herstellers (nur indirekt, falls in techn. Unterlagen erwähnt — Edge-Case)

Out-of-Scope

- **Webseite-Besucher-Tracking** — ce-doc.eu setzt keine personalisierten Cookies, keine Web-Analytics mit Personenbezug. Separat in `datenschutz.html`.
- **Allgemeines DSGVO-Compliance-Audit** — siehe AUDIT-01 (TOM-Bericht).
- **Sub-Verarbeiter-Bewertung** — siehe AUDIT-06 Cross-Provider-Privacy.
- **Krankheits-/Gesundheits-Daten** — werden architektonisch ausgeschlossen (keine Felder im Schema vorgesehen).

Schnittstellen zu anderen Audit-Aspekten

Bezug	Aspekt
TOMs zur Risikominderung	AUDIT-01 + AVV-Anlage B
Sub-Verarbeiter-Kette	AUDIT-06
Verfügbarkeit + Datenpannen-Reaktion	AUDIT-05 + PROC-K3
Tenant-Isolation als Vertraulichkeits-Garantie	AUDIT-11 (neu)
Forensische Reproduzierbarkeit für Auskunfts-/Lösch-Rechte	AUDIT-12 (neu)

Bezugsnormen / Bezugswerke

- DSGVO Art. 35 (DPIA-Pflicht), Art. 36 (Konsultations-Pflicht), Erw.gr. 84/89–96
- EDPB Guidelines 4/2017 + WP 248 (DPIA-Methodik)
- CNIL „PIA: methodology" + „PIA: knowledge bases" (operative Vorlage)
- BSI-Standard 200-3 (Risiko-Analyse als Schadens-/Wahrscheinlichkeits-Matrix)
- BayLDA-Liste verarbeitungspflichtiger Tätigkeiten („Muss-Liste")