AUDIT-08 — Controls (Anbieter-DPIA für CE-Doc-Pipeline)

Stand: 2026-05-18 **Methodik:** CNIL/BSI-200-3, Schadensschwere × Eintrittswahrscheinlichkeit, Bewertung vor + nach Mitigation

1. Beschreibung der Verarbeitung

Aspekt	Antwort
Verarbeitungs-Zweck	Erstellung CE-konformer technischer Unterlagen nach EU-MV 2023/1230
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragserfüllung) zwischen Koordinator und Hersteller; wir sind nach Art. 28 Auftragsverarbeiter
Datenarten	siehe 01_scope.md Tabelle
Empfänger	Sub-Verarbeiter laut Verfahrensverzeichnis + öffentliche `vertraulichkeit.html`
Drittland-Transfer	nur in Ausnahmefällen (Anthropic-Fallback): SCC + Art. 28+46
Speicherdauer	10 Jahre nach Maschinen-Inverkehrbringen (MV-Pflicht) bzw. nach Vertragsende

2. Verhältnismäßigkeit + Notwendigkeit (CNIL „Proportionality")

Frage	Antwort	Status
Ist die Verarbeitung verhältnismäßig zum Zweck?	Ja — wir verarbeiten nur, was für die CE-Akte gebraucht wird. Pipeline filtert aktiv, was nicht im Schema vorgesehen ist.	✓
Datenminimierung umgesetzt?	Ja — keine Telemetrie auf Person, anonymisierte Logs (AUD-1 Sprint KW 24–25 für Live-Daten)	◐
Speicherbegrenzung?	Ja — automatische Cache-Löschung nach 30 Tagen, Workspace-Lifecycle nach Vertragsende	✓
Zweckbindung?	Ja — kein KI-Training auf Mandantendaten, vertraglich + architektonisch (siehe AVV § 4 + 7)	✓
Transparenz?		✓

Frage	Antwort	Status
	Ja — Hersteller wird über Koordinator + AVV informiert, Sub-Verarbeiter-Liste öffentlich	
Betroffenen-Rechte umsetzbar?	Auskunft + Berichtigung + Löschung Art. 15–17: ja, Schnittstelle über Koordinator (AVV § 6)	✓

3. Risiken für Betroffene (BSI-200-3-Matrix)

Schwere: 1 = vernachlässigbar, 2 = begrenzt, 3 = erheblich, 4 = maximal
Wahrscheinlichkeit: 1 = vernachlässigbar, 2 = begrenzt, 3 = erheblich, 4 = maximal

R-1 Unberechtigter Daten-Zugriff (Vertraulichkeitsverlust)

Aspekt	Vor Mitigation	Nach Mitigation
Schwere	3 (Betriebsgeheimnis)	3
Wahrscheinlichkeit	3	1
Quelle	Cyber-Angriff, Insider, Tenant-Bruch	dito
Mitigation	Bastion-Host, 2FA, Verschlüsselung in-transit (TLS 1.3) + at-rest (LUKS, AUD-5 in Arbeit), Tenant-Isolation (AUDIT-11), No-Training-Klauseln in Sub-AVVs	
Restrisiko	begrenzt-akzeptabel	

R-2 Daten-Verfälschung (Integritätsverlust)

Aspekt	Vor	Nach
Schwere	3 (falsche CE-Akte → Haftungs-Risiko Koordinator)	3
Wahrscheinlichkeit	3	1
Mitigation	CM-1-SHA-256-Stempel (AUDIT-12), Versions-Diff, Append-only Audit-Trail, Vier-Augen-Freigabe-Gate, Lektor-L4-Konsistenz-Check	
Restrisiko	begrenzt	

R-3 Daten-Verlust (Verfügbarkeits-Verlust)

Aspekt	Vor	Nach
Schwere	2	2
Wahrscheinlichkeit	3	1

Aspekt	Vor	Nach
Mitigation	3-Tier-Backup (täglich 30d + wöchentlich 12M + monatlich 5J), DR Helsinki↔Frankfurt RTO 4h / RPO 24h, 10-Jahres-Archiv mit Hash-Stempel	
Restrisiko	gering	

R-4 Unzulässige Weiterverarbeitung (Zweck-Verletzung)

Aspekt	Vor	Nach
Schwere	4 (KI-Training mit fremden Daten ohne Berechtigung)	4
Wahrscheinlichkeit	2 (Provider-Default)	1
Mitigation	No-Training-Klauseln in Mistral-/Anthropic-DPAs; Workshop-Verbote in `core/skills/llm/*`; Switchboard-Filter im Prompt-Pfad gegen versehentliches Forwarding; quartalsweises Provider-AGB-Audit (PROC-K2)	
Restrisiko	gering-akzeptabel	

R-5 Diskriminierende KI-Aussage

Aspekt	Vor	Nach
Schwere	2 (technische Akte, kaum Diskriminierungs-Potential)	2
Wahrscheinlichkeit	2	1
Mitigation	KI-VO-Transparenz-Header je Akte; Vier-Augen-Freigabe macht Koordinator zum Letzt-Entscheider; Modell-Provenance dokumentiert	
Restrisiko	gering	

R-6 Datenpanne mit Nicht-Meldung (Compliance-Verlust)

Aspekt	Vor	Nach
Schwere	3 (Bußgeld bis 4 % Konzernumsatz, hier irrelevant — und vor allem Reputations-Schaden)	3
Wahrscheinlichkeit	2	1
Mitigation	PROC-K3 Incident-Response mit 72-h-Eskalation an BayLDA; klar dokumentierte Stufen P0..P3; KPI 100 % rechtzeitige Meldung	
Restrisiko	gering	

4. Konsultations-Pflicht (Art. 36)

Nach Bewertung der Restrisiken nach Mitigation ist **keines** auf „erheblich" oder höher (Schwere × Wahrscheinlichkeit). Eine vorgängige Konsultation der Aufsichtsbehörde nach Art. 36 ist daher **nicht erforderlich**.

Bei künftiger Erweiterung um Hochrisiko-KI-Anwendungen nach EU AI Act Anhang III (z. B. Personalentscheidungen, biometrische Identifikation) wäre die Konsultation zwingend — was wir architektonisch ausschließen (kein solcher Use Case im Scope).

5. Ergebnis

Die Pipeline-Verarbeitung ist DSGVO-konform durchführbar. Sechs identifizierte Risiken sind dokumentiert und durch konkrete Mitigationen auf akzeptables Niveau reduziert. Drei HIGH-Befunde sind in Umsetzung (AUD-1 PII-Log-Filter, AUD-5 At-rest-Verschlüsselung, AUD-8 Archivierungs-Service), siehe `04_findings.md` und `../_BEFUND_DASHBOARD.md`.