

AUDIT-08 — Review-Log

Konvention: Append-only.

Initial-Lauf 2026-05-18

Auditor: R-COMP **Audit-Form:** Anbieter-DPIA + Koordinator-Vorlagen-Erstellung

Methodik: CNIL/BSI-200-3 Schadens-/Wahrscheinlichkeits-Matrix; sechs Risiken identifiziert **Dauer:** ca. 4 h Methodik + Befüllung + Koordinator-Vorlage

Bewertung

Die Anbieter-DPIA ist strukturell vollständig. Sechs Risiken sind bewertet, mit Mitigationen versehen und im Befund-Dashboard verfolgt. Drei der Mitigationen (PII-Anonymisierung, At-rest-Verschlüsselung, Archiv-Service) sind sprintgeplant für KW 24-25; bis zur Fertigstellung wird der Pilot-Lauf mit erhöhter manueller Überwachung geführt.

Die Koordinator-DPIA-Vorlage ([dpia_vorlage_berater.md](#)) ist als CNIL-PIA-strukturiertes Dokument verfügbar mit pre-befüllten Antworten für die wiederkehrenden Pipeline-spezifischen Fragen. Der Koordinator muss nur noch fünf Pflicht-Felder selbst befüllen (Mandanten-Identität, Maschinen-Typ, betroffene Hersteller-Mitarbeiter-Zahl, eigene IT-Umgebung, eigene Versicherung).

Empfehlung

1. Pilot-Koordinator bekommt das DPIA-Pack ([dpia_vorlage_berater.md](#)) als Bestandteil des Onboarding-Mappes (PROC-K1 Schritt „Kick-Off-Mail“).
2. Validierung der Vorlage mit dem ersten Pilot-Mandanten Q3 2026.
3. Nach Validierung: Vorlage in [docs/governance/contracts/](#) als zweite Konversions-relevante Vorlage neben AVV-Muster.

Nächster Lauf

- Nach Schließung der drei HIGH-Befunde: Re-Audit KW 28
- Nach Pilot-Validierung der Koordinator-Vorlage: Vorlage-Revision
- Jahres-Review: 2027-05-18