

AUDIT-08 — Datenschutz-Folgenabschätzung (DPIA)

Trägerorganisation: EcoHub München GmbH, Produktlinie CE-Doc / AIMOS **Aktueller Stand:** Anbieter-DPIA strukturell vollständig; Koordinator-Vorlage einsatzbereit; drei HIGH-Befunde gekoppelt mit dem Code-Sprint KW 24-25/2026 **Letzter Lauf:** 2026-05-18 (Initial-Befüllung) **Nächster Lauf:** Nach Schließung der HIGH-Befunde sowie pro Pilot-Mandant

Inhalt

Das Bündel umfasst zwei Bestandteile:

- 1. Anbieter-DPIA — eigene Datenschutz-Folgenabschätzung der CE-Doc-Pipeline nach CNIL/BSI-Methodik, dokumentiert in `02_controls.md` und `03_evidence.md`.
- 2. Koordinator-Vorlage (`dpia_vorlage_berater.md`) — für die DPIA-Pflicht des Koordinators nach DSGVO Art. 35 vorausgefüllt; fünf Felder bleiben durch den Koordinator zu ergänzen (Mandanten-Identität, Maschinen-Typ, betroffene Hersteller-Mitarbeiter, eigene IT-Umgebung, eigene Versicherung).

Datei-Übersicht

Datei	Inhalt	ca. Lesezeit
<code>00_policy.md</code>	Selbstverpflichtung	1 min
<code>01_scope.md</code>	Datenkategorien und Verarbeitungstätigkeiten	3 min
<code>02_controls.md</code>	CNIL/BSI-Methodik; sechs Risiken bewertet	6 min
<code>03_evidence.md</code>	Belege und Stichproben	3 min
<code>04_findings.md</code>	Sechs Befunde, davon drei HIGH (Duplikate AUD-1/-5/-8)	2 min
<code>05_review_log.md</code>	Audit-Bericht (append-only)	3 min
<code>dpia_vorlage_berater.md</code>	Vorlage für den Koordinator	8 min

Befund-Status

ID	Schwere	Status	Anmerkung
AUDIT-08-F-01	HIGH	offen, KW 24-25/2026	Duplikat AUD-1 (Log-PII-Filter)
AUDIT-08-F-02	HIGH	offen, KW 24-25/2026	Duplikat AUD-5 (At-rest-Verschlüsselung)
AUDIT-08-F-03	HIGH	offen, KW 24-25/2026	Duplikat AUD-8 (Archivierungs-Service)
AUDIT-08-F-04	MED	offen, Q3/2026	Quartalsweises Provider-Audit, Erst-Durchführung
AUDIT-08-F-05	LOW	offen, 2026-08-17	Datenpannen-Tabletop-Drill
AUDIT-08-F-06	LOW	offen, Q3/2026	Pilot-Validierung der Koordinator-Vorlage

Bezug zu anderen Audit-Aspekten

Bezug	Aspekt
TOMs	AUDIT-01 und AVV Anlage B
Sub-Verarbeiter	AUDIT-06
Tenant-Isolation	AUDIT-11
Reproduzierbarkeit, 10-Jahres-Archiv	AUDIT-12