

AUDIT-08 — DPIA (Datenschutz-Folgenabschätzung)

Aspekt: Datenschutz-Folgenabschätzung nach DSGVO Art. 35 **Norm-Basis:** DSGVO Art. 35 + CNIL-Methodik (PIA Knowledge Bases) + BSI-Standard 200-3 (Risiko-Analyse) + EDPB Guidelines 4/2017 **Stand:** 2026-05-18 (Initial-Befüllung) **Verantwortlich:** R-COMP, mit fachlichem Input des Pilot-Koordinators **Reife-Stand:** ✓ Anbieter-DPIA strukturell vollständig; ● Pilot-Befüllung mit erstem produktiven Koordinator

Selbstverpflichtung

Die EcoHub München GmbH bekennt sich zu zwei separierten DPIA-Pflichten und liefert die dazu erforderliche Dokumentation:

1. **Anbieter-DPIA** (in unserer Rolle als Auftragsverarbeiter nach Art. 28): Wir führen eine eigene Datenschutz-Folgenabschätzung für die CE-Doc- Pipeline durch und legen sie offen. Das vereinfacht Mandanten-Verträge.
2. **Koordinator-DPIA-Vorlage:** Da der CE-Koordinator als Verantwortlicher selbst nach Art. 35 DPIA-pflichtig ist, sobald er KI-gestützt Hersteller-Daten verarbeitet, stellen wir ihm eine vorausgefüllte Vorlage zur Verfügung ([dpia_vorlage_berater.md](#)).

Geltungsbereich

- CE-Doc-Pipeline-Verarbeitung von Hersteller-Daten (Stammdaten, technische Unterlagen, Koordinator-Kommunikation, OPL-Antworten)
- Sub-Verarbeiter-Kette (Mistral, Anthropic, Hetzner, Mailbox.org, Ionos)
- Koordinator-Portal mit eigenen Mandanten-Vorgängen
- Mail-Bridge IMAP/SMTP

Außerhalb: rein-öffentliche Inhalte (Norm-Texte, anonymisierte Demo-Akten); deren Verarbeitung berührt keine personenbezogenen Daten.

Bezugsdokumente

- [01_scope.md](#) — Genauer Scope mit Datenkategorien
- [02_controls.md](#) — Methodik + Risiko-Bewertung
- [03_evidence.md](#) — Belege (TOMs, AVV, Verfahrensverzeichnis)
- [04_findings.md](#) — Offene Restrisiken + Mitigation
- [05_review_log.md](#) — Audit-Historie (append-only)
- [dpia_vorlage_berater.md](#) — **Vorlage für den Koordinator**, pre-befüllt für CE-Doc-Einsatz