

DPIA-Vorlage für CE-Koordinator — CE-Doc / AIMOS-Einsatz

Zweck: Vorlage zur Erfüllung Ihrer eigenen DPIA-Pflicht nach DSGVO Art. 35, wenn Sie CE-Doc / AIMOS als KI-gestütztes Werkzeug für die Erstellung technischer Unterlagen Ihrer Hersteller-Mandanten einsetzen.

Methodik: CNIL „PIA: methodology“ + EDPB Guidelines 4/2017 **Stand der Vorlage:** 2026-05-18 **Format:** Fünf Pflicht-Felder müssen Sie selbst befüllen ([POL] markiert). Den Rest haben wir pre-befüllt — bitte prüfen + ggf. anpassen.

Hinweis zur Verwendung

Diese Vorlage wandert nach Befüllung in Ihre eigene Datenschutz-Akte. Wir empfehlen einmalige Befüllung pro Mandanten-Beziehung (nicht pro Vorgang), mit Aktualisierung bei wesentlicher Änderung der Verarbeitungs-Lage. Die Vorlage ist nicht als Vertrag zu verstehen — der vertragliche Teil läuft über NDA + AVV separat.

Teil A — Verarbeitungs-Beschreibung

A.1 Verantwortlicher

[POL] Tragen Sie hier Ihre Koordinator-Identität ein: - Koordinator-Name / Firma: - Geschäftsanschrift: - Datenschutz-Kontakt (i. d. R. Sie selbst): - Ggf. bestellter externer DSB:

A.2 Auftragsverarbeiter

- **Name:** EcoHub München GmbH
- **Sitz:** Ohlenschlagerstraße 14, 81369 München
- **Geschäftsführerin:** Müge Fuchsenberger
- **AVV-Stand:** unterzeichnet am [Datum aus eigenem AVV]
- **Sub-Verarbeiter:** Mistral AI (FR), Anthropic (US, SCC), Hetzner (DE), Mailbox.org (DE), Ionos (DE) — Liste öffentlich auf [vertraulichkeit.html](https://www.ionos.de/vertraulichkeit.html)

A.3 Verarbeitungs-Zweck

Erstellung CE-konformer technischer Unterlagen für Maschinen-Hersteller-Mandanten nach EU-Maschinenverordnung 2023/1230, einschließlich Risikobewertung, Konformitätsanalyse, Norm-Compliance, Wartungs- und Betriebsanleitungs- Bestandteilen.

A.4 Rechtsgrundlage

- **Art. 6 Abs. 1 lit. b DSGVO** (Vertragserfüllung) zwischen Ihnen und Ihrem Hersteller-Mandanten
- **Art. 28 DSGVO** für die Verarbeitung durch EcoHub München GmbH (AVV abgeschlossen)
- **MV 2023/1230** als sektorale Rechtsgrundlage für die 10-Jahres-Aufbewahrung

A.5 Datenarten

Kategorie	Erfasst	Schutzklasse
Hersteller-Stammdaten (Firma, USt-ID, Geschäftsführer)	✓	normal
Technische Unterlagen (Stückliste, Schaltplan, Risiko-Bewertung)	✓	erhöht (Betriebsgeheimnis)
Konstrukteur-/Sicherheitsingenieur-Namen (in Dokumenten-Headern)	gelegentlich	normal
OPL-Klärungs-Mails inkl. Mail-Adressen Hersteller-Mitarbeiter	✓	normal
Koordinator-Notizen, interne Vermerke	✓	normal
Art-9-Sonderkategorien (Gesundheit, biometrisch etc.)	nein	n/a

A.6 Betroffene Personen

- Hersteller-Mitarbeiter (Geschäftsführer, Konstrukteure, Sicherheits-Ingenieure)
- **[POL]** Tragen Sie hier die geschätzte Anzahl Personen pro Mandanten ein. Beispiel: „typisch 3-8 Personen pro Maschinen-Akte“.

A.7 Speicherdauer

- 10 Jahre nach Inverkehrbringen der Maschine (MV-Pflicht)
- Bei Vertragsende: Workspace-Export an Sie (verschlüsseltes ZIP mit SHA-256-Hash), danach kryptografische Löschung beim Auftragsverarbeiter
- Sub-Verarbeiter-Logs (LLM-Provider): 7 Tage (Mistral), 30 Tage (Anthropic)

A.8 Empfänger

- EcoHub München GmbH (Auftragsverarbeiter laut AVV)
- Sub-Verarbeiter laut A.2
- Auf Anfrage des Hersteller-Mandanten: Marktüberwachungsbehörde

Teil B — Verhältnismäßigkeit + Notwendigkeit

B.1 Ist die KI-gestützte Verarbeitung verhältnismäßig?

Ja. Die CE-Doc-Pipeline ersetzt **keine** Koordinator-Tätigkeit, sondern beschleunigt sie. Vier-Augen-Prinzip ist architektonisch erzwungen: jede Akte muss vom Koordinator (Ihnen) freigegeben werden, bevor sie als „final“ gilt. Die Verarbeitung ist auf das beschränkt, was die EU-MV ohnehin als technische-Unterlagen-Pflicht verlangt — keine Profilbildung, keine automatisierte Einzelentscheidung mit Rechtswirkung im Sinne von Art. 22.

B.2 Datenminimierung

- Keine Telemetrie auf Person
- Keine Profilbildung der Hersteller-Mitarbeiter
- Keine Verwendung der Hersteller-Daten für KI-Training (vertraglich + architektonisch)
- Pipeline-Logs werden nach 30 Tagen automatisch gelöscht (Cache-Lifecycle)

B.3 Zweckbindung

Die Verarbeitung ist auf die CE-Akte-Erstellung beschränkt. Keine Verwendung der Daten für andere Zwecke. **No-Training-Klauseln** in den Sub-AVV's mit Mistral und Anthropic. Workspace-Isolation pro Mandant verhindert Kreuz-Verwertung.

B.4 Transparenz

- Hersteller wird über Sie als Koordinator informiert (Sie sind Verantwortlicher)
- Sub-Verarbeiter-Liste öffentlich
- KI-VO-Transparenz-Header in jeder erstellten Akte gemäß KI-VO Art. 50

B.5 Betroffenen-Rechte (Art. 15-22 umsetzbar?)

Recht	Umsetzungs-Pfad
Auskunft Art. 15	Anfrage geht an Sie (Verantwortlicher); Sie erhalten von uns einen Workspace-Auszug binnen 5 Werktagen
Berichtigung Art. 16	Sie können falsche Stammdaten im Portal jederzeit korrigieren
Löschung Art. 17	Anfrage geht an Sie; Sie veranlassen Offboarding bei uns (PROC-K1); MV-Aufbewahrungspflicht 10 J kann Löschung blockieren
Einschränkung Art. 18	Portal-Sperre des Vorgangs möglich
Übertragbarkeit Art. 20	Workspace-Export verschlüsselt + maschinenlesbar
Widerspruch Art. 21	n/a (Rechtsgrundlage Vertrag, nicht Interesse)
Automatisierte Entscheidung Art. 22	nicht einschlägig — Vier-Augen-Koordinator-Freigabe konstitutiv

Teil C — Risiken + Mitigationen

Wir haben unsere eigenen sechs Risiken in der [Anbieter-DPIA](#) bewertet und sie mit Mitigationen versehen. **Für Ihre DPIA übernehmen Sie diese Bewertung sinngemäß** — Sie tragen die koordinator-spezifischen Restrisiken zusätzlich ein:

C.1 Risiken aus dem Pipeline-Einsatz (aus Anbieter-DPIA)

ID	Risiko	Schwere × W'lichkeit nach Mitigation	Mitigation (kurz)
R-1	Vertraulichkeitsverlust	3 × 1	Bastion, 2FA, Tenant-Isolation, No-Training
R-2	Integritätsverlust	3 × 1	CM-1-Stempel, Versions-Diff, Vier-Augen
R-3	Verfügbarkeitsverlust	2 × 1	3-Tier-Backup, DR Helsinki↔Frankfurt
R-4	Zweck-Verletzung	4 × 1	No-Training in Sub-AVV's, Quartals-Audit
R-5	Diskriminierende KI-Aussage	2 × 1	Vier-Augen-Prinzip, KI-VO-Header
R-6	Datenpanne ohne Meldung	3 × 1	PROC-K3, 72-h-BayLDA-Eskalation

C.2 Koordinator-spezifische Zusatz-Risiken

[POL] Bewerten Sie hier Restrisiken, die wir **nicht** abdecken können:

ID	Risiko	Schwere	W'lichkeit	Mitigation durch Sie
B-1	Eigene IT-Umgebung (Koordinator-Laptop) kompromittiert	[POL]	[POL]	[POL: eigene Schutz-Maßnahmen]
B-2	Eigene Mail-Konten unsicher (z. B. Hersteller-Mail-Versand)	[POL]	[POL]	[POL: SPF/DKIM/DMARC, 2FA, Mail-Provider]
B-3	Versehentliche Mandanten-Verwechslung im Portal	[POL]	[POL]	[POL: eigene Bearbeitungs-Disziplin]
B-4	Verletzung der MV-10-J-Aufbewahrungspflicht	[POL]	[POL]	[POL: eigene Geschäftsfortführungs-Regelung]

ID	Risiko	Schwere	W'lichkeit	Mitigation durch Sie
	durch Koordinator-Wegfall			
B-5	Eigene Berufshaftpflicht-Lücke	[POL]	[POL]	[POL: siehe POL-10_haftung_und_versicherung.md für unsere Empfehlung]

Teil D — Konsultations-Pflicht (Art. 36)

Nach Bewertung aller Risiken nach Mitigation ist **kein** Restrisiko auf „erheblich oder höher“ (Schwere × W'lichkeit nach EDPB) — Vorgängige Konsultation der bayerischen Aufsicht (BayLDA) **nicht erforderlich**.

Hinweis: Sollten Sie selbst zusätzliche Hochrisiko-Verarbeitungen betreiben (z. B. biometrische Identifikation, KI-Personalentscheidungen Anhang III EU AI Act), gilt diese Bewertung NICHT — dann müssen Sie eine separate DPIA für diese Verarbeitungen führen.

Teil E — Schlussbewertung

- ☐ Verhältnismäßigkeit gegeben
- ☐ Datenminimierung umgesetzt
- ☐ Zweckbindung gewährleistet
- ☐ Transparenz hergestellt
- ☐ Betroffenen-Rechte umsetzbar
- ☐ Restrisiken auf akzeptables Niveau reduziert
- ☐ Keine vorgängige Konsultation Art. 36 erforderlich

Unterschrift Verantwortlicher (Koordinator):

Name (Druckbuchstaben)

Ort, Datum

Unterschrift Verantwortlicher

Datum nächster Review (i. d. R. jährlich oder bei wesentlicher Änderung):

Anhang — Was wir Ihnen für die Befüllung liefern können

Wenn Sie Unterstützung beim Befüllen der [POL]-Felder brauchen, fragen Sie unter dpia@ce-doc.eu. Wir liefern auf Anfrage: 1. Letztes Self-Audit-Pack (ISO 9001 + DSGVO TOM + DPIA) als PDF 2. Bestätigung Tenant-Isolation (AUDIT-11) für Ihre Bewertung von B-3 3. Forensische-Reproduzierbarkeits-Bestätigung (AUDIT-12) für B-4 4. Versicherungs-Empfehlung (POL-10) für B-5

Diese Vorlage ersetzt keine Rechtsberatung. Im Zweifel: Datenschutz-Juristen oder Aufsichtsbehörde konsultieren.