Vorlage Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Vorbefüllte Vorlage für Ihre Datenschutz-Folgenabschätzung, Stand 22. Oktober 2026. Eine Folgenabschätzung ist jedenfalls beim Modul Task Mining angezeigt (Art. 35 Abs. 1 DSGVO; DSK-Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist). Die Verantwortung für die Bewertung liegt bei Ihnen als Verantwortlichem. Bitte mit Ihrer Datenschutzbeauftragten abstimmen.

1. Beschreibung der Verarbeitung

- **Zweck:** Analyse von Geschäftsabläufen (Verkauf, Einkauf, Reklamation, weitere Prozesse), Erkennung und Klärung von Vorgängen mit Klärungsbedarf, Ursachenanalyse, Prognose von Terminrisiken je Vorgang, Vorschläge zur Behebung. Optional Task Mining: Bildschirmzeit je freigegebener Anwendung und Prozessschritt auf Teamebene.
- **Datenquellen:** ERP (Aufträge, Bestellungen, Lieferungen, Rechnungen, Zahlungen, Stammdaten), Sammelpostfächer, optional CRM, IT-Service-Management und Data Warehouse, optional Browsererweiterung und Desktop-Agent für Task Mining.
- **Betroffene:** Ansprechpartner bei Kunden und Lieferanten (Geschäftskontakte), Beschäftigte der beteiligten Bereiche (nur pseudonymisiert oder als Team, beim Task Mining über zufällige Gerätekennungen).
- **Empfänger:** CoreGnition UG als Auftragsverarbeiter; Unterauftragsverarbeiter Hetzner Online GmbH (Hosting und Sicherung in Deutschland), Brevo GmbH (Systemmails), Mistral AI SAS (Sprachmodell, Verarbeitung in der EU, ohne Training mit Kundendaten). Alternativ ohne Sprachmodell.

2. Rechtsgrundlagen

- Kundenkontakte: Art. 6 Abs. 1 lit. b und f DSGVO (Vertragsabwicklung, berechtigtes Interesse an effizienter Auftragsbearbeitung).
- Beschäftigte: Art. 6 Abs. 1 lit. b und f DSGVO, ergänzend eine Betriebsvereinbarung als Kollektivvereinbarung nach Art. 88 DSGVO. Hinweise: Nach EuGH, Urteil vom 30.03.2023 (C-34/21), ist § 26 Abs. 1 Satz 1 BDSG als eigenständige Rechtsgrundlage zweifelhaft. Nach EuGH, Urteil vom 19.12.2024 (C-65/23), müssen Betriebsvereinbarungen die Anforderungen der DSGVO vollständig erfüllen. Nach BAG, Urteil vom 08.05.2025 (8 AZR 209/21), kann eine Verarbeitung über das Erforderliche hinaus einen Schadensersatz nach Art. 82 DSGVO auslösen, auch wenn sie in einer Betriebsvereinbarung vorgesehen ist. Für Tests und Einrichtung daher nur die nötigen Daten verwenden.

3. Notwendigkeit und Verhältnismäßigkeit

- Auswertung auf Ebene von Aufträgen, nicht von Personen.

- Pseudonymisierung von Beschäftigten mit einem geheimen Schlüssel je Kundeninstanz; Benutzerkonten nur für Administratoren sichtbar.
- k-Anonymität (mindestens fünf Fälle je Gruppe).
- Löschung von Mailtexten nach 90 Tagen, von Task-Mining-Sitzungen nach 180 Tagen.
- Task Mining nur für freigegebene Anwendungen, ohne Inhalte, Titel, Adressen oder Eingaben, Auswertung erst ab fünf Geräten je Team, Pause jederzeit möglich.
- Nur lesender Zugriff auf Quellsysteme im Standardbetrieb; Änderungen im ERP nur nach Freigabe.

4. Risiken und Maßnahmen

Risiko	Bewertung vor Maßnahmen	Maßnahme	Restrisiko
Rückschluss auf einzelne Beschäftigte	mittel	Pseudonym, Team-Ebene, k-Anonymität, keine Personenkennzahlen	gering
Unbefugter Zugriff auf Mailinhalte	mittel	Rollenrechte, Verschlüsselung, Namensmaskierung, 90-Tage-Löschung	gering
Fehlerhafte KI-Vorschläge	mittel	Belege je Angabe, Konfidenz, Freigabepflicht, Prüfprotokoll	gering
Datenabfluss außerhalb der EU	gering	EU-Hosting, EU-Sprachmodell oder lokales Modell wählbar	gering
Zweckänderung (Leistungskontrolle)	mittel	keine Personenkennzahlen in der Software, Betriebsvereinbarung § 3	gering
Task Mining: Rückschluss auf einzelne Beschäftigte	hoch	nur freigegebene Anwendungen, keine Inhalte, monatlich wechselnde Gerätekennung, Mindestgröße fünf Geräte, Löschung nach 180 Tagen, Pause, Anlage 3 der Betriebsvereinbarung	gering bis mittel, abhängig von der Teamgröße
Task Mining: Druck durch Messung	mittel	Erprobungsphase mit gemeinsamer Auswertung, Information vor dem Start, keine Folgen bei Pause	gering

5. Ergebnis

Nach Umsetzung der Maßnahmen verbleibt nach Einschätzung des Anbieters ein geringes Risiko, beim Task Mining abhängig von der Teamgröße. [Durch den Verantwortlichen zu bewerten und zu bestätigen. Datum, Beteiligung der Datenschutzbeauftragten, Überprüfungstermin.]