Technische und organisatorische Maßnahmen (TOM)

Anlage 1 zum Vertrag zur Auftragsverarbeitung und Grundlage für Anlage 1 der Betriebsvereinbarung, Stand 22. Oktober 2026. Gegliedert nach Art. 32 Abs. 1 DSGVO. Ein Informationssicherheits-Managementsystem nach ISO/IEC 27001 ist im Aufbau, eine Zertifizierung ist noch nicht erfolgt.

1. Daten zu Beschäftigten

Feld	Inhalt	Zweck
Benutzerkonto	Anmeldename, Rolle, Gruppen; bei automatischer Übernahme aus dem Identitätssystem (SCIM) dessen Angaben, etwa der Anzeigename	Anmeldung und Rechtevergabe, nur für Administratoren sichtbar
Pseudonym	z. B. MA-3F2A, berechnet mit SHA-256 und einem geheimen Schlüssel je Kundeninstanz	Nachvollziehbarkeit von Freigaben ohne Klarnamen
Team	z. B. Team Süd	Auswertung auf Teamebene
Gerätekennung (nur Task Mining)	Zufallswert, auf dem Gerät erzeugt, wechselt monatlich, in Ordyse nur als Prüfsumme gespeichert	Mindestgröße von fünf Geräten je Team
Sitzung (nur Task Mining)	Kennung der freigegebenen Anwendung, Beginn, Dauer	Bildschirmzeit je Prozessschritt und Team

Nicht gespeichert: Bearbeitungszeiten je Person, Bildschirminhalte, Fenstertitel, Adressen, Tastatur- oder Mauseingaben, Anwesenheit. In Prozessdaten, Auswertungen und Protokollen erscheinen keine Klarnamen.

2. Vertraulichkeit

- **Zutritt:** Betrieb in Rechenzentren der Hetzner Online GmbH in Deutschland mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal; Hetzner ist nach ISO/IEC 27001 zertifiziert. Der Anbieter unterhält keine eigenen Serverräume.
- **Zugang:** Verwaltung der Server nur über verschlüsselte Verbindungen durch den Anbieter; Anmeldung der Nutzer per Einmal-Link und Code oder über das Identitätssystem des Kunden (zum Beispiel Microsoft Entra ID).
- **Zugriff:** rollenbasierte Rechte nach dem Grundsatz der Erforderlichkeit; Rolle „Betriebsrat“ nur lesend auf Einstellungen und Protokolle; Fragen in Alltagssprache nur auf Sichten ohne Personenbezug.
- **Trennung:** eigene Datenbank je Kunde; Zugangsdaten zu ERP und Postfach verschlüsselt gespeichert, Schlüssel getrennt von den Daten.

- **Pseudonymisierung:** Beschäftigte nur als Pseudonym und Team; Personennamen in E-Mails maskiert; Auswertungen erst ab fünf Fällen je Gruppe.
- **Verschlüsselung:** TLS 1.2 oder höher bei jeder Übertragung; Verschlüsselung gespeicherter Zugangsdaten.

3. Integrität

- Protokoll aller Freigaben, Importe, Exporte und Änderungen an Einstellungen, mit Pseudonym und Zeitpunkt.
- Lesender Zugriff auf Quellsysteme im Standardbetrieb; Änderungen im ERP und Mails nach außen nur nach Freigabe durch eine berechtigte Person, auf Wunsch durch eine zweite Person.
- Der Ordyse-Agent für SAP ECC liest mit einem RFC-Benutzer nur lesend, baut nur ausgehende Verbindungen auf und überträgt nur die vereinbarten Belegtabellen.

4. Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbanken in einen Objektspeicher bei Hetzner in Deutschland, Aufbewahrung 14 Sicherungen, zusätzlich tägliche Abbilder des Servers.
- Die Dienste laufen in Containern, die nach einem Ausfall automatisch neu starten.
- Wiederherstellung aus der Sicherung; der Anbieter prüft die Wiederherstellung regelmäßig.

5. Datensparsamkeit und Löschung

- Mailtexte nach 90 Tagen automatisch gelöscht (täglicher Lauf); Betreff, Zeitpunkt und extrahierte Angaben ohne Personenbezug bleiben.
- Task-Mining-Sitzungen nach 180 Tagen gelöscht.
- Ohne anschließenden Tarif: Löschung der angebundenen Daten spätestens 60 Tage nach dem Ergebnisbericht der Prozessanalyse.
- Nach Vertragsende: Export in offenen Formaten (OCEL 2.0, CSV), danach vollständige Löschung nach § 10 AVV, auf Wunsch mit Bestätigung.

6. KI-Komponenten

- Sprachmodell von Mistral AI über den EU-Endpunkt, nur zustandslose Aufrufe, kein Training mit Kundendaten.
- Übermittelt werden nur die Inhalte, die die jeweilige Aufgabe braucht.
- Alternativ ohne Sprachmodell regelbasiert oder mit einem Modell im Netz des Kunden.

7. Task Mining (nur mit Anlage 3 der Betriebsvereinbarung)

- Erfassung nur freigegebener Anwendungen; Vergleich von Fenstertiteln nur auf dem Gerät, nie übertragen.
- Übertragung per TLS mit einem Schlüssel je Team, der jederzeit entzogen werden kann.
- Auswertung nur für Teams ab fünf Geräten; Pause jederzeit möglich, ohne dass sie erfasst wird.

8. Organisation und Überprüfung

- Verpflichtung aller Personen mit Zugriff auf Vertraulichkeit und Datenschutz.
- Verfahren für Datenschutzverletzungen mit Meldung an den Kunden innerhalb von 48 Stunden (§ 8 Abs. 3 AVV).
- Auswahl und vertragliche Bindung der Unterauftragsverarbeiter nach Art. 28 Abs. 4 DSGVO.
- Überprüfung dieser Maßnahmen mindestens einmal im Jahr und bei wesentlichen Änderungen am Produkt (Art. 32 Abs. 1 lit. d DSGVO).