Technical and organizational measures (TOMs)

This English version is a convenience translation. In the event of any discrepancy, the German version shall prevail.

Annex 1 to the data processing agreement and basis for Annex 1 of the works council agreement, as of October 22, 2026. Structured according to Art. 32(1) GDPR. An information security management system in accordance with ISO/IEC 27001 is being set up; certification has not yet taken place.

1. Employee data

Field	Content	Purpose
User account	Login name, role, groups; for automatic provisioning from the identity system (SCIM), its attributes, such as the display name	Sign-in and assignment of permissions, visible to administrators only
Pseudonym	E.g. MA-3F2A, calculated with SHA-256 and a secret key per customer instance	Traceability of approvals without real names
Team	E.g. Team South	Analysis at team level
Device ID (task mining only)	Random value generated on the device, changes monthly, stored in Ordyse only as a hash	Minimum size of five devices per team
Session (task mining only)	ID of the approved application, start, duration	Screen time per process step and team

Not stored: handling times per person, screen content, window titles, addresses, keyboard or mouse input, attendance. No real names appear in process data, analyses or logs.

2. Confidentiality

- **Physical access control:** Operation in data centers of Hetzner Online GmbH in Germany with access control, video surveillance and security staff; Hetzner is certified to ISO/IEC 27001. The provider does not maintain its own server rooms.
- **System access control:** Server administration only by the provider via encrypted connections; user sign-in via one-time link and code or via the customer's identity system (for example Microsoft Entra ID).
- **Data access control:** Role-based permissions on a need-to-know basis; the "Works council" role has read-only access to settings and logs; questions in everyday language only on views without personal reference.
- **Separation:** A separate database per customer; credentials for ERP and mailbox stored encrypted, with keys kept separate from the data.

- **Pseudonymization:** Employees only as pseudonym and team; personal names masked in emails; analyses only for groups of at least five cases.
- **Encryption:** TLS 1.2 or higher for every transmission; encryption of stored credentials.

3. Integrity

- Log of all approvals, imports, exports and changes to settings, with pseudonym and timestamp.
- Read-only access to source systems in standard operation; changes in the ERP and outgoing emails only after approval by an authorized person, or by a second person if requested.
- The Ordyse agent for SAP ECC reads with a read-only RFC user, only establishes outbound connections and only transmits the agreed document tables.

4. Availability and resilience

- Daily backup of the databases to object storage at Hetzner in Germany, retention of 14 backups, plus daily server snapshots.
- Services run in containers that restart automatically after a failure.
- Restoration from backup; the provider tests restoration regularly.

5. Data minimization and deletion

- Email texts deleted automatically after 90 days (daily job); subject, time and extracted information without personal reference are retained.
- Task mining sessions deleted after 180 days.
- Without a subsequent plan: deletion of the connected data at the latest 60 days after the results report of the process analysis.
- After the end of the contract: export in open formats (OCEL 2.0, CSV), followed by complete deletion in accordance with § 10 of the DPA, with confirmation upon request.

6. AI components

- Language model from Mistral AI via the EU endpoint, stateless calls only, no training on customer data.
- Only the content required for the respective task is transmitted.
- Alternatively rule-based without a language model, or with a model in the customer's network.

7. Task mining (only with Annex 3 of the works council agreement)

- Recording of approved applications only; window titles are compared on the device only and never transmitted.
- Transmission via TLS with a key per team that can be revoked at any time.
- Analysis only for teams with five or more devices; pause possible at any time without being recorded.

8. Organization and review

- All persons with access are bound to confidentiality and data protection.

- Procedure for personal data breaches with notification to the customer within 48 hours (§ 8(3) of the DPA).
- Selection and contractual commitment of sub-processors in accordance with Art. 28(4) GDPR.
- Review of these measures at least once a year and in the event of material changes to the product (Art. 32(1)(d) GDPR).