Data protection impact assessment template (Art. 35 GDPR)

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

Pre-filled template for your data protection impact assessment (DPIA), as of October 22, 2026. A DPIA is in any case indicated for the Task mining module (Art. 35(1) GDPR; list of processing operations requiring a DPIA published by the German Data Protection Conference (DSK)). As the controller, you are responsible for the assessment. Please coordinate with your data protection officer.

1. Description of the processing

- **Purpose:** Analysis of business processes (sales, purchasing, complaints, other processes), detection and resolution of cases requiring clarification, root cause analysis, forecasting of deadline risks per case, proposals for remediation. Optionally task mining: screen time per approved application and process step at team level.
- **Data sources:** ERP (sales orders, purchase orders, deliveries, invoices, payments, master data), shared mailboxes, optionally CRM, IT service management and data warehouse, optionally a browser extension and desktop agent for task mining.
- **Data subjects:** Contact persons at customers and suppliers (business contacts), employees of the departments involved (only pseudonymized or as a team, for task mining via random device IDs).
- **Recipients:** CoreGnition UG as processor; sub-processors Hetzner Online GmbH (hosting and backup in Germany), Brevo GmbH (system emails), Mistral AI SAS (language model, processing in the EU, no training on customer data). Alternatively without a language model.

2. Legal bases

- Customer contacts: Art. 6(1)(b) and (f) GDPR (performance of contracts, legitimate interest in efficient order processing).
- Employees: Art. 6(1)(b) and (f) GDPR, supplemented by a works council agreement as a collective agreement under Art. 88 GDPR. Notes: According to the CJEU judgment of March 30, 2023 (C-34/21), § 26(1), first sentence, of the German Federal Data Protection Act (BDSG) is questionable as an independent legal basis. According to the CJEU judgment of December 19, 2024 (C-65/23), works council agreements must fully comply with the requirements of the GDPR. According to the Federal Labour Court (BAG) judgment of May 8, 2025 (8 AZR 209/21), processing beyond what is necessary may give rise to damages under Art. 82 GDPR, even if it is provided for in a works council agreement. For testing and setup, therefore use only the data that is needed.

3. Necessity and proportionality

- Analysis at the level of sales orders, not persons.

- Pseudonymization of employees with a secret key per customer instance; user accounts visible to administrators only.
- k-anonymity (at least five cases per group).
- Deletion of email texts after 90 days and of task mining sessions after 180 days.
- Task mining only for approved applications, without content, titles, addresses or input, analysis only for teams of at least five devices, pause possible at any time.
- Read-only access to source systems in standard operation; changes in the ERP only after approval.

4. Risks and measures

Risk	Assessment before measures	Measure	Residual risk
Inferences about individual employees	medium	Pseudonym, team level, k-anonymity, no per-person metrics	low
Unauthorized access to email content	medium	Role-based permissions, encryption, name masking, deletion after 90 days	low
Incorrect AI proposals	medium	Source document per item of information, confidence, approval requirement, audit log	low
Data leaving the EU	low	EU hosting, EU language model or local model selectable	low
Change of purpose (performance monitoring)	medium	No per-person metrics in the software, works council agreement § 3	low
Task mining: inferences about individual employees	high	Only approved applications, no content, device ID changing monthly, minimum size of five devices, deletion after 180 days, pause, Annex 3 of the works council agreement	low to medium, depending on team size
Task mining: pressure from measurement	medium	Pilot phase with joint evaluation, information before the start, no consequences for pausing	low

5. Result

After implementation of the measures, in the provider's assessment a low risk remains, for task mining depending on team size. [To be assessed and confirmed by the controller. Date, involvement of the data protection officer, review date.]