Works council agreement template (Germany) for the use of Ordyse

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

This template is intended for companies in Germany that have a works council (Betriebsrat). Under the German Works Constitution Act (Betriebsverfassungsgesetz, BetrVG), introducing software such as Ordyse is subject to co-determination by the works council. Companies without a works council do not need this agreement; the employee information notice and the data protection documents still apply.

Template to prepare discussions with the works council, as of October 22, 2026. Not a substitute for legal advice. Please adapt it to the circumstances of your establishment and have it reviewed under employment and data protection law before signing. Square brackets mark items you fill in or select.

The following works council agreement is concluded between **[Company]**, represented by its management (hereinafter the "Employer"), and the **Works Council of [Company]** (hereinafter the "Works Council").

§ 1 Subject matter and scope

1. This agreement governs the introduction, use and further development of the Ordyse software (provider: CoreGnition UG (haftungsbeschränkt), Munich) in the establishment **[establishment/sites]**.
2. Ordyse is used in the following areas: **[inside sales, credit management, purchasing, accounts payable, accounts receivable, complaint management, materials planning, master data maintenance]**.
3. It applies to all employees within the meaning of § 5(1) BetrVG whose work generates data processed by Ordyse. Executive employees within the meaning of § 5(3) BetrVG are not treated differently.
4. This agreement governs co-determination under § 87(1) no. 6 BetrVG. The parties assume that Ordyse is objectively capable of generating data that allow conclusions to be drawn about conduct or performance; an intention to monitor is irrelevant. The rights of the Works Council under §§ 80, 90 and 87(1) no. 1 BetrVG remain unaffected.
5. The modules of Ordyse are described in Annex 1. The **Task mining** module is only used if the parties have separately signed Annex 3. Without Annex 3, task mining is not permitted.

§ 2 Purpose

1. Ordyse serves exclusively to make business processes visible (for example order to delivery, purchase to payment, complaint to resolution), to identify delays and their root causes, to support the handling of cases and to permanently eliminate recurring root causes.
2. The subject of analysis is business transactions and documents (sales orders, purchase orders, deliveries, invoices, payments, complaints, service cases), customers, suppliers, items, master data and process steps. **Employees are not the subject of analysis.**
3. Use for any other purpose is only permitted with the prior consent of the Works Council (§ 9).

§ 3 Excluded uses

The following uses are excluded. Where the software prevents them technically, this is described in Annex 1.

1. Monitoring of the performance and conduct of individual employees, including rankings, handling times, case counts or error rates per person.
2. Analyses, metrics, automations, custom apps or questions to the data that relate to individual employees or to groups of fewer than five persons.
3. Recording of keystrokes, mouse movements, screen content, screenshots, window titles, visited addresses or file names. For the Task mining module, only the exhaustive provisions in Annex 3 apply.
4. Monitoring of attendance, breaks or start and end of work.
5. Emotion recognition, analysis of personality traits or moods (cf. Art. 5(1)(f) AI Act).
6. Automated decisions concerning employees within the meaning of Art. 22 GDPR.
7. Linking data from Ordyse with other employee data (for example time recording, personnel files, access control) in order to draw conclusions about individual persons.
8. Use of data from Ordyse for employment law measures against individual employees. Data obtained in breach of this agreement will not be used to the detriment of employees.

§ 4 Legal basis and data protection

1. The processing of employees' personal data is based on Art. 6(1)(b) and (f) GDPR. This agreement is a collective agreement within the meaning of Art. 88 GDPR. It specifies the processing and creates additional safeguards. It does not establish any processing that would not already be permissible under Art. 5, Art. 6(1) and Art. 9(1) GDPR, and it does not replace the assessment of whether processing is necessary (CJEU, judgment of December 19, 2024, C-65/23; Federal Labour Court (BAG), judgment of May 8, 2025, 8 AZR 209/21).
2. Before the introduction, the Employer carries out a data protection impact assessment pursuant to Art. 35 GDPR, at least for the Task mining module, and makes it available to the Works Council. The data protection officer is involved.
3. The provider processes the data as a processor pursuant to Art. 28 GDPR on the basis of a data processing agreement. The data are processed on servers in Germany. Sub-processors are listed in Annex 2 of the data processing agreement; the Employer informs the Works Council of any changes.
4. Employees are informed pursuant to Art. 13 GDPR before use (Annex 4).

§ 5 Data processed and retention periods

1. In process data, analyses and logs, employees are processed exclusively as a **pseudonym** (for example "MA-3F2A") and by **team membership**. The pseudonym is calculated with a secret key per customer instance. For sign-in, Ordyse maintains user accounts with login name, role and groups, which only administrators can see. Pseudonyms may only be attributed to persons in accordance with § 6(3).
2. From connected systems (ERP, mailbox, CRM, IT service management, data warehouse), Ordyse only takes over the handling team or group for process steps, not names or user IDs.
3. Analyses are carried out exclusively at the level of teams, customers, suppliers, items and root causes. The software combines groups with fewer than **five** cases. Teams with fewer than **five** persons are not set up as a separate team in Annex 2 but are assigned to a larger team.
4. Email texts are stored only to display the document in the respective case. Personal names are masked in the display unless they are needed for handling the case. Email texts in the Ordyse inbox and outbox are deleted after **90 days**. Subject, time and extracted information without personal reference (for example order number, price, date) are retained. Retention of business correspondence is governed by the Employer's systems (for example the mailbox), not by Ordyse.
5. The audit log (approvals, changes to settings, imports, exports) is retained for **[24 months]** and then deleted, unless a statutory retention obligation applies.
6. Annex 1 contains an overview of all data fields relating to employees.

§ 6 Proposals, approval and automations

1. Proposals made by Ordyse (for example an email to a customer, a query to a supplier, a change in the ERP system) are only executed once an authorized person has approved them.
2. Automations and actions in custom apps report cases as a task, by email or via webhooks to collaboration tools (for example Microsoft Teams). They relate to cases and metrics, not to persons. For actions with external effect, approval by a second person can be set up.
3. Approvals are recorded in the audit log. The audit log serves to make business transactions traceable and is not used to monitor performance or conduct. Analyzing the audit log by person is only permitted to investigate a specific security incident or a suspicion of misuse, after prior notification of the Works Council.

§ 7 Forecasts and language models

1. Forecasts in Ordyse relate to cases (for example: "This delivery will probably miss its due date"), not to employees. Attributes relating to employees or teams are not used for forecasts insofar as they allow conclusions to be drawn about individual persons.
2. A language model may be used for drafting text, analyzing emails and answering questions in everyday language. It is operated in the EU, and the model provider does not use the data for training. Questions to the data only read approved views without personal reference.
3. In the provider's assessment, Ordyse in the agreed use is not a high-risk AI system within the meaning of Annex III no. 4 of the AI Act (classification in the annex "EU AI Act classification"). If the use changes, the classification is reviewed again before the change and the Works Council is informed.

§ 8 Access rights

1. The roles listed in Annex 2 are given access to Ordyse. Rights are granted on a need-to-know basis.
2. The Works Council receives read-only access with the role "Works council". With it, the Works Council sees the settings under "Privacy", the audit log, the connections and, for the Task mining module, the approved applications. The role does not see any business data.

§ 9 Changes and extensions

1. The following require the prior consent of the Works Council: new modules, new data sources containing employee data, changes to the limits in §§ 3 and 5, for task mining any change to the approved applications (Annex 3a) and any reduction of the minimum team size.
2. New processes, metrics, automations and custom apps that relate only to business transactions and comply with the limits of this agreement do not require separate consent. The Employer informs the Works Council about them **[quarterly]** in text form.
3. The Employer notifies the Works Council of provider updates that change the safeguards described in Annex 1 before they are used.

§ 10 Training

Employees who use Ordyse are trained before use. The training covers the purpose, functionality, limits of proposals and forecasts, the approval requirement and the handling of AI results (AI literacy pursuant to Art. 4 AI Act).

§ 11 Oversight

The Works Council may verify compliance with this agreement at any time. For this purpose, the Employer provides the system documentation, the data protection impact assessment and the settings. The Works Council may consult an expert in accordance with § 80(3) BetrVG.

§ 12 Entry into force and termination

1. This agreement enters into force upon signature. It may be terminated with three months' notice to the end of a month. It continues to apply until a new agreement is concluded.
2. Annex 3 (Task mining) may be terminated separately with the same notice period. When Annex 3 ends, the task mining components are uninstalled and the recorded sessions are deleted within 30 days.
3. Should any provision be invalid, the remainder of the agreement remains valid. The parties replace the provision with one that comes closest to its purpose.

[Place], [Date]

_____ (Employer) _____ (Works Council)

Annex 1: Modules, data fields and safeguards

Module	What it does	Employee data
Process analysis	Process map, variants, target flow comparison, throughput time, root causes, bottlenecks, comparison	Team per process step
Forecast and simulation	Risk per case for a deadline, effect of an improvement	none
Apps	Work lists with proposals for order resolution, invoice verification, receivables, delivery dates, complaints	Pseudonym for approvals
Custom apps	Self-configured work lists with actions	Pseudonym for actions and approvals
Cockpit, metrics, automations	Metrics on cases, notifications when thresholds are reached	none
Questions to the data	Answers from approved views without personal reference	none
Task mining (only with Annex 3)	Screen time per approved application and process step, per team	Random device ID, team

Field	Content	Purpose
User account	Login name, role, groups, and the display name if taken over from the identity system	Sign-in and permissions, visible to administrators only
Pseudonym	For example MA-3F2A, calculated with a secret key per customer instance	Traceability of approvals
Team	For example Technical purchasing	Analysis at team level
Device ID (task mining only)	Random value generated on the device, changes every month	Counting devices per team for the minimum size

Technically implemented safeguards: no per-person metrics in the software, minimum size of five cases per group and five devices per team for task mining, name masking in emails, deletion of email texts after 90 days and of task mining sessions after 180 days, questions only on views without personal reference, approval requirement for actions with external effect.

Annex 2: Roles and access rights

[List of roles from the portal under "Roles and permissions", for example Management, Sales clerk, Purchasing clerk, Accounting, Admin, Works council (read-only), with the assignment of groups from Microsoft Entra ID.]

Annex 3: Task mining module

1. **Purpose.** Task mining determines how much on-screen working time is spent in which process step in order to simplify workflows, avoid duplicate work and plan automation. It does not serve to assess employees.
2. **Applications recorded.** Only the applications exhaustively listed in Annex 3a (web addresses and program files) are recorded. All other applications and websites are neither recorded nor reported.
3. **Data recorded.** Per session: ID of the approved application, start, duration in seconds. In addition, team membership via the team key and a random device ID that is generated on the device and changes every month.
4. **Not recorded.** Content, window titles, addresses, file names, keystrokes, mouse movements, screenshots, user name, computer name. If a window title text has been agreed for an application (for example the name of an SAP transaction), it is only compared on the device and never transmitted.
5. **Idle time.** No time is recorded if there is no keyboard or mouse input for two minutes.
6. **Analysis.** Analyses only show teams with at least **five** devices. Smaller teams are hidden. Analysis by device or person is not provided for and is not permitted.
7. **Information and pause.** Employees are informed before the first start (Annex 4). A notice that must be confirmed appears on the first start. Recording can be paused at any time. Use of the pause function is not recorded and has no consequences.
8. **Retention period.** Sessions are deleted after **180 days**.
9. **Distribution.** IT distributes the browser extension and desktop agent centrally. Team keys are only given to IT and can be revoked at any time.
10. **Pilot.** Task mining is initially piloted for **[three months]** in the teams **[teams]**. The Employer and the Works Council then evaluate the pilot together and decide whether to continue.

Annex 3a: Approved applications

Type	Address or program	Window title text (optional)	Application	Process step
Browser	[erp.company.com/sap/bc/ui5_ui5]		[SAP Fiori]	[Invoice approved]
Desktop	[saplogon.exe]	[Blocked invoices]	[SAP GUI]	[Block released]
Desktop	[excel.exe]		[Excel]	[Reconciliation in Excel]

Annex 4: Information for employees

See the template "Employee information notice".