document: 03 · Data Processing Agreement (DPA) — Art. 28 GDPR version: draft v0.1 date: 06.08.2026 issuer: CIBINNO CONSULTING S.R.L.

DATA PROCESSING AGREEMENT (DPA)

concluded under **Article 28 of Regulation (EU) 2016/679 (GDPR)** and **Romanian Law no. 190/2018**, as an integral annex to the related SaaS Licensing and Services Agreement (number and date — completed upon signature of the Agreement).

English courtesy translation. The Romanian version of this document is the legally binding reference; in case of any discrepancy, the Romanian version prevails.

THE PARTIES

The Controller: CIBINNO CONSULTING S.R.L., tax ID RO51836516, registered office JUD. ILFOV, ORŞ. PANTELIMON, STR. VATRA DORNEI, NR.3, represented by Cosmin Balaban — determines the purposes and means of the processing (Art. 4(7) GDPR).

The Processor: CIBINNO CONSULTING S.R.L., VAT no. 51836516, registered office Ilfov County, Pantelimon, Str. Vatra Dornei no. 3, represented by Cosmin Ionut Balaban — processes Personal Data on behalf of the Controller (Art. 4(8) GDPR).

ARTICLE 1 — SUBJECT MATTER AND DURATION

1.1. The Processor processes Personal Data on behalf of the Controller exclusively for the provision of the CIBINNO AI Platform and related services, in accordance with the Agreement.

1.2. The duration of the processing matches the term of the Agreement. Upon termination, Article 10 (deletion/return) applies.

1.3. The details of the processing (categories of data subjects, categories of data, operations, purposes) are set out in **Annex I**. Sub-processors are listed in **Annex II**. The technical and organisational measures (Art. 32) are set out in **Annex III**.

ARTICLE 2 — THE CONTROLLER'S INSTRUCTIONS

2.1. The Processor processes the Data **only on documented instructions** from the Controller (Art. 28(3)(a) GDPR), including with regard to international transfers. The Agreement, this DPA, the Approved Scoping and the Controller's configuration of the Platform constitute such instructions.

2.2. The Processor informs the Controller if, in its opinion, an instruction infringes the GDPR or other applicable rules (Art. 28(3), final sentence).

2.3. The Processor does not process the Data for its own purposes. ⚠ Use of the AI Assistant (Module X) does not entail training models on the Controller's Data unless this is contractually excluded with the LLM Sub-processor; see Article 6 and Annex II.

ARTICLE 3 — CONFIDENTIALITY OF PERSONNEL

3.1. The Processor ensures that persons authorised to process the Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR).

ARTICLE 4 — SECURITY OF PROCESSING (ART. 32)

4.1. The Processor implements technical and organisational measures appropriate to the risk, in accordance with **Art. 32 GDPR**, detailed in **Annex III**, including, as applicable: pseudonymisation/encryption, confidentiality, integrity, availability and resilience, restoration after an incident, periodic testing/evaluation.

4.2. The measures rely on the Microsoft Azure infrastructure (Sub-processor) and on the Platform's own controls (RBAC, audit journal, tenant isolation).

ARTICLE 5 — RBAC, LOGGING AND MONITORING

5.1. Access to the Data is granted on the basis of RBAC Roles. The audit journal records accesses and operations, with a retention of at least 12 months, in accordance with the **Access Monitoring Notice** (`04-access-monitoring-notice.md`).

5.2. Access monitoring serves security (Art. 32) and legitimate interest (Art. 6(1)(f)); it is not used for any other purpose.

ARTICLE 6 — SUB-PROCESSORS (ART. 28(2) AND (4))

6.1. The Controller gives a **general authorisation** for the use of Sub-processors, with the Processor's obligation to inform the Controller of any intended addition or replacement, allowing **14 days** for reasoned objections.

6.2. The Sub-processors agreed as at the date of signature are those listed in **Annex II**, in particular: (a) **Microsoft Azure** (hosting/infrastructure) — region West Europe, within the EEA; (b) the **LLM Sub-processor** Anthropic (Claude) — regiune Frankfurt (Germania), în UE, jurisdiction UE — Frankfurt (Germania) — for processing AI Assistant queries.

6.3. The Processor imposes on each Sub-processor, by contract, **the same data-protection obligations** as those set out in this DPA (Art. 28(4)).

ARTICLE 7 — INTERNATIONAL TRANSFERS

7.1. Data are transferred outside the EEA only if: (a) an adequacy decision exists (Art. 45); or (b) appropriate safeguards are in place (Art. 46), in particular **SCCs**; or (c) a derogation applies (Art. 49).

7.2. If the AI Assistant involves a transfer outside the EEA, the Parties conclude/ incorporate **SCCs** and, where necessary, supplementary measures, in accordance with **Annex II**. Nu se aplică — toți Subîmputerniciții prelucrează exclusiv în UE/SEE.

7.3. If all Sub-processors (including the LLM) are located within the EEA, this Article does not apply to transfers.

ARTICLE 8 — ASSISTANCE TO THE CONTROLLER

8.1. **Data subject rights (Art. 28(3)(e)).** The Processor assists the Controller, by appropriate technical and organisational measures, in responding to requests for the exercise of data subject rights (access, rectification, erasure, restriction, portability, objection), insofar as this is possible. The export/deletion functions of the Platform serve this purpose.

8.2. **Compliance support (Art. 28(3)(f)).** The Processor assists the Controller in complying with the obligations under Articles 32–36 GDPR (security, breach notification, DPIA, prior consultation of the supervisory authority), taking into account the nature of the processing and the information available.

ARTICLE 9 — NOTIFICATION OF PERSONAL DATA BREACHES

9.1. The Processor notifies the Controller **without undue delay**, and in any case no later than **48 hours** after becoming aware of a Personal Data Breach (Art. 33(2) GDPR).

9.2. The notification includes, to the extent available: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed.

9.3. The Processor cooperates with and supports the Controller in handling the breach and in any notification to the supervisory authority (ANSPDCP) and to the data subjects.

ARTICLE 10 — DELETION OR RETURN OF DATA

10.1. Upon termination of the provision of services, at the Controller's choice, the Processor **returns** or **deletes** all Data and copies, save for those the retention of which is required by law (Art. 28(3)(g) GDPR).

10.2. Export: on request, in a structured, commonly used, machine-readable format, within 30 days. Deletion: within 30 days of export/termination, including from backups in accordance with their normal rotation cycle.

ARTICLE 11 — AUDITS AND INSPECTIONS

11.1. The Processor makes available to the Controller the information necessary to demonstrate compliance with Art. 28 and allows for audits, including inspections, conducted by the Controller or by a mandated auditor (Art. 28(3)(h)).

11.2. Audits are carried out with reasonable prior notice (10 days), during business hours, without affecting the security of other tenants, and may be satisfied by making available reports/certifications (e.g. those of Azure) where these cover the subject matter of the audit.

ARTICLE 12 — LIABILITY

12.1. Liability in matters of data protection is established in accordance with Art. 82 GDPR and is aligned with the caps set out in the Agreement (Art. 13), within the mandatory limits of the law.

ARTICLE 13 — FINAL PROVISIONS

13.1. In the event of a conflict between this DPA and the Agreement on data-protection matters, this DPA prevails.

13.2. Governing law: Romanian law and the GDPR. Electronic signature (eIDAS) accepted.

SIGNATURES

Controller — CIBINNO CONSULTING S.R.L.	**Processor — CIBINNO CONSULTING S.R.L.**
Cosmin Balaban	Cosmin Ionut Balaban, Administrator
Electronic signature (eIDAS)	Electronic signature (eIDAS)
Date: 06.08.2026	Date: 06.08.2026

ANNEX I — DETAILS OF THE PROCESSING

Nature and purpose of the processing: provision of the CIBINNO AI Platform (hosting, ERP integration through Connectors, visualisation/analysis, AI assistant, audit), for the purpose of the Beneficiary's operational management.

Duration: for the term of the Agreement; audit journals — minimum 12 months.

Categories of data subjects: the Beneficiary's Users; representatives/contact persons of the Beneficiary's customers and suppliers; the Beneficiary's employees (including drivers, warehouse operators, sales agents); where applicable, other persons whose data reside in the ERP.

Categories of personal data, by Module (only the Modules activated in the Approved Scoping are processed):

Module	Categories of personal data
I. Executive Cockpit	Mainly aggregated data/KPIs; possibly names of Users/agents in reports
II. Sales/CRM/Quoting	Name, position, e-mail, phone of customer representatives; identity of sales agents; interaction history
III. Purchasing/ Procurement	Contact details of supplier representatives; identity of procurement officers
IV. Inventory/ Warehouses/WMS	Identity of warehouse operators (who scanned/operated), timestamps
V. Logistics/Fleet/GPS	Identity of drivers; **GPS location data** associated with drivers/ vehicles; telemetry
VI. Projects/Sites	Identity of field workers; **GPS-tagged photographs**; signatures (including those of the works' beneficiaries)
VII. Finance/Treasury/ Cashflow	Mainly company financial data; possibly names in transactions/ approvals
VIII. HR	**Personnel data: name, position, salary/payroll data, timekeeping/leave**; CNP/IBAN — doar în Modulul HR, dacă e activat — ⚠ **assess whether special categories (Art. 9) occur**
IX. Legal/Compliance	Data from files/registers, identity of the persons involved; audit journals
X. AI Assistant	Content of queries (may incidentally include personal data from the other Modules); identity of the User
XI. Mobile/Field/Offline	Identity of field operators; GPS photographs; signatures; location
XII. Administration/ RBAC/Connectors/Audit	User accounts (authentication identifier, e-mail), **IP addresses**, audit journal (who/what/when), access configurations

Operations: collection (through Connectors from the ERP/third parties), storage, organisation, structuring, consultation, use, aggregation/analysis, processing through the LLM (Module X), export, deletion.

⚠ **Special categories (Art. 9):** by design, the Platform does **not** aim to process special categories of data. If the ERP/HR data flow incidentally includes such data, the Controller informs the Processor and supplementary measures are agreed.

ANNEX II — LIST OF SUB-PROCESSORS

Sub-processor	Service	Jurisdiction / region	Transfer outside the EEA	Safeguard (if applicable)
Microsoft (Azure)	Hosting, infrastructure, backup	UE — West Europe	Nu	Microsoft DPA / Microsoft standard SCCs
Anthropic (Claude) — regiune Frankfurt (Germania), în UE	Processing of AI Assistant queries (Module X)	UE — Frankfurt (Germania)	Nu	No training on the Controller's Data; processing in the EU
Microsoft 365 (Graph)	E-mail / collaboration (Email/Teams Module), if activated	UE — West Europe	Nu	Microsoft DPA / Microsoft standard SCCs

ANNEX III — TECHNICAL AND ORGANISATIONAL MEASURES (ART. 32)

A. Access and identity control - Named authentication of Users; MFA (multi-factor authentication): Da. - Role-based access control (RBAC); "need-to-know" principle; per-tenant isolation. - Administrative access restricted to authorised CIBINNO personnel, and logged.

B. Encryption - Encryption in transit (TLS) and criptare la repaus (prin Azure Storage).

C. Logging and monitoring - Audit journal of accesses and operations; retention ≥ 12 months. - Abuse detection (failed authentications, anomalous patterns), in accordance with the Monitoring Notice.

D. Availability and resilience - Periodic backup (frequency zilnic, retention 30 zile), restore testing. - Resilience through the Azure infrastructure.

E. Security of development and operations - Separation of environments (dev/test/prod); secrets management; security updates. - Minimisation of the use of real data in non-production environments.

F. Organisational measures - Confidentiality commitments of personnel. - Breach management procedure; point of contact. - Sub-processor management (due diligence, Art. 28 contracts).

G. Data protection contact person at CIBINNO: contact@cibinno.ro.