GDPR ART. 28 · DATA PROCESSING AGREEMENT

Data Processing Agreement (DPA)

This Agreement sets the terms for processing personal data under the GNDLF Ctrl-Cost service and forms an integral part of the main Service Agreement.

CONTROLLER

Customer

The individual or entity identified in the main Service Agreement/order.

PROCESSOR

Cloud Solutions for Business Sweden AB

Box 4004, 169 04 Solna, Stockholm, Sweden · VAT no: SE559056482801 · info@gndlf.io

Version date: 31.08.2026

1. Definitions & Roles

In this Agreement "GDPR" means Regulation (EU) 2016/679; "personal data", "processing", "controller", "processor" and "data subject" have the meanings given in the GDPR.

The parties agree that for processing under this Agreement the **Customer is the controller** and **GNDLF is the processor**. In case of conflict between this Agreement and the main Service Agreement, this Agreement prevails as to personal data protection.

2. Subject Matter, Duration & Purpose

The subject matter, nature, purpose, categories of personal data and categories of data subjects are set out in **Annex I**. Processing continues for as long as the main Service Agreement is in force.

3. Controller Instructions

GNDLF processes personal data only on the Customer's **documented instructions** (including this Agreement and the main Service Agreement). Use of the Service constitutes such instructions.

If GNDLF believes an instruction infringes data protection law, it will inform the Customer. GNDLF does not use the data for its own purposes and does not sell it to third parties.

4. Processor Obligations

GNDLF will: (a) ensure personnel accessing personal data are under a duty of confidentiality; (b) limit access to personnel who need it to provide the Service, on a least-privilege basis; (c) implement appropriate technical and organizational measures under Art. 32 (**Annex II**); and (d) make available reasonable information to demonstrate compliance with this Agreement.

5. Security (Art. 32)

GNDLF implements the technical and organizational measures listed in **Annex II** to ensure a level of security appropriate to the risk (encryption in transit, access control, tenant isolation, read-only SAP

access, etc.). Measures may be updated to reflect technical progress; updates will not lower the level of protection.

6. Sub-processors

The Customer gives general authorization for GNDLF to engage the sub-processors listed in **Annex III**. GNDLF imposes on each sub-processor, by contract, data protection obligations materially the same as those in this Agreement, and remains liable to the Customer for the sub-processor's compliance.

GNDLF will give reasonable prior notice of adding or replacing a sub-processor; the Customer may object on reasonable data protection grounds.

7. Assistance with Data Subject Rights

Taking into account the nature of the processing, GNDLF will assist the Customer by appropriate technical and organizational measures, insofar as possible, to respond to data subject requests under GDPR Chapter III (access, rectification, erasure, restriction, portability, objection). Requests received directly by GNDLF are forwarded to the Customer without undue delay.

8. Personal Data Breach Notification

GNDLF will notify the Customer **without undue delay — and, where reasonably practicable, within 24 hours** — after becoming aware of a personal data breach and will provide reasonable information to enable the Customer to meet its notification obligations to the supervisory authority and/or data subjects.

9. DPIA & Prior Consultation Assistance

Taking into account the nature of processing and information available to it, GNDLF will provide reasonable assistance to the Customer with data protection impact assessments (DPIAs) and, where required, prior consultation with the supervisory authority.

10. International Transfers

Personal data is, as a rule, processed within the EU/EEA. If a transfer outside the EU/EEA is required, GNDLF will ensure a valid transfer mechanism under GDPR Chapter V (adequacy decision or standard contractual clauses — SCCs) is in place.

11. Deletion or Return

After the end of the Service, GNDLF will, at the Customer's choice, **delete or return** the personal data within 30 days, unless EU/Member-State law requires storage. Personal data in routine backup systems is securely overwritten or deleted in line with the backup lifecycle and is not restored except for disaster recovery. In an on-premises deployment the data already resides on the Customer's server.

12. Audit

GNDLF will make available information necessary to demonstrate compliance with this Agreement and will allow for and contribute to audits conducted by the Customer (or an independent auditor it mandates). Audits take place **at most once per year** (except in case of a security incident), on at least **30 days' written**

notice, at the Customer's cost, during business hours and without disrupting operations; no access to other customers' data is permitted and all findings are subject to confidentiality.

13. Liability & Governing Law

The parties' liability is subject to the limitations in the main Service Agreement. **GNDLF's aggregate liability arising out of or in connection with this Agreement shall not exceed the liability cap set out in the main Service Agreement and shall not include indirect, incidental or consequential damages (including loss of profit).** This Agreement is governed by **Swedish law**; the courts of Stockholm have jurisdiction. Mandatory provisions of the GDPR are reserved.

14. Effectiveness

This Agreement takes effect on acceptance of the main Service Agreement and applies for as long as processing continues. Questions: info@gndlf.io.

ANNEX I

Processing Details

- **Subject matter:** provision of the GNDLF Ctrl-Cost SAP License Intelligence service.
- **Duration:** the term of the main Service Agreement.
- **Nature & purpose:** analysis of SAP license usage; classification of users by real usage; over/under-licensing reporting; audit readiness. Processing is read-only.
- **Categories of data subjects:** the Customer's SAP users/employees; the Customer's authorized contacts.
- **Categories of personal data:** user IDs, usernames, name, work email, role, and the SAP transaction/license usage information necessary for license optimization and audit readiness.
- **Special categories:** none. The Customer undertakes not to provide special-category personal data to the Service unless expressly agreed in writing.

ANNEX II

Technical & Organizational Measures (TOMs)

- TLS encryption in transit.
- Hashed passwords (scrypt); signed cookies for sessions.
- Role-based access control and least-privilege.
- **Tenant isolation** in the multi-tenant environment; customer data kept separate.
- **Read-only** SAP access — nothing is written to any system.
- In-product (dashboard) AI runs in a controlled/on-prem model; run data is not sent to a third-party cloud model for that purpose.
- Access logging; regular backups; breach response process.
- Confidentiality obligations and awareness for personnel.

ANNEX III

Approved Sub-processors

SUB-PROCESSOR	PURPOSE	LOCATION
Brevo	Email delivery (notifications, confirmations)	EU
Hostinger	Website hosting	EU
Hetzner	Application hosting	Germany (EU)
OpenRouter	Website chat assistant only	USA

No customer SAP data or customer personal data processed through Ctrl-Cost is transferred to the AI provider; the provider is used only for the public website chat assistant.

Signatures

CONTROLLER (CUSTOMER)

Name

Title

Date

Signature

PROCESSOR

Cloud Solutions for Business Sweden AB

Name

Title

Date

Signature