DATA PROCESSING ADDENDUM (DPA)

Last Updated: July 28, 2026

Parties: Incorporated automatically as Annex A to the Customer Agreement between **AISolutions AS** (Org. nr: 931 884 220) ("Data Processor") and the **Customer** ("Data Controller").

1. Purpose and Scope

1.1. This Data Processing Addendum ("DPA") governs the Processing of Personal Data by the Data Processor on behalf of the Data Controller in connection with the delivery of cloud-based AI and automation services (including AidEun, SalesQuote, and associated platforms).

1.2. This DPA shall ensure that Personal Data is processed in compliance with the European General Data Protection Regulation (GDPR Art. 28) and applicable Norwegian data protection legislation.

2. Nature, Purpose, and Duration of Processing

2.1. **Purpose:** Processing shall strictly occur to deliver, operate, automate, and support the Services pursuant to the Customer Agreement.

2.2. **Categories of Data Subjects:** Customer’s employees, recipients of customer end-documents, email correspondents, and primary contact persons.

2.3. **Types of Personal Data:** Names, email addresses, contact details, free text/prompts in emails and quotations, system audit logs, and access credentials.

2.4. **Duration:** This DPA remains effective for as long as the Customer Agreement is active and terminates once all Personal Data has been deleted or returned.

2.5. **Storage & Configurable Retention:** Personal Data is retained only as long as necessary for the purposes in 2.1. The Data Controller may configure standard retention periods directly within the Service settings (default 12 months for conversation logs, configurable between 30 days and 24 months; default 24 months for RFQ records, configurable to 12, 24, or 36 months). Custom retention periods outside standard parameters require Privacy Lead approval. In all cases, termination of the Customer Agreement overrides retention settings and triggers prompt deletion or return per Section 3(f).

3. Obligations of the Data Processor (GDPR Art. 28)

The Data Processor covenants and agrees to:

- **a. Instructions:** Process Personal Data solely on documented written instructions from the Data Controller, including with regard to transfers of personal data to a third country.
- **b. Confidentiality:** Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- **c. Technical Security (Art. 32):** Implement appropriate technical and organizational security measures in alignment with ISO 27001 standards (including encryption of data in transit and at rest, Role-Based Access Control, Multi-Factor Authentication, and continuous logging).
- **d. Assistance with Data Subject Rights:** Assist the Data Controller by appropriate technical and organizational measures in fulfilling its obligations to respond to requests for exercising data subjects' rights (access, erasure, rectification).
- **e. Incident Notification (Art. 33/34):** Notify the Data Controller without undue delay after becoming aware of a personal data breach or security incident affecting Customer Personal Data.
- **f. Deletion or Return:** At the choice of the Data Controller, delete or return all Personal Data upon termination of services within 90 days, unless applicable law requires retention.
- **g. Audits and Compliance:** Make available to the Data Controller all information necessary to demonstrate compliance with GDPR Art. 28 obligations (e.g., by providing ISO 27001 certificates or SOC 2 summaries).

4. Special Terms for AI Processing and Model Training

4.1. **No Base Model Training:** The Data Processor guarantees that Personal Data, prompts, email content, or documents processed via external AI model endpoints (e.g., OpenAI API) are **not** utilized by AI model providers to train, fine-tune, or improve their base models.

4.2. **Ephemeral Processing:** AI prompts and inference payloads are processed ephemerally, the published page is updated, and customers are notified of the material change in 3(f).

5. Sub-processors and Disclosure

5.1. The Data Controller grants general written authorization for the Data Processor to engage sub-processors to deliver and support the Services.

5.2. An up-to-date, comprehensive list of all authorized sub-processors, including their locations, processing purposes, and transfer mechanisms, is maintained and publicly disclosed at:

👉 **https://www.aisolutions.no/suppliers**

5.3. **Notification of Changes:** The Data Processor shall notify the Data Controller (via email or website announcement) at least 15 days prior to adding or replacing any sub-processor. The Data Controller retains the right to object to such changes on reasonable, documented data protection grounds.

6. International Data Transfers

Transfers or remote access to data from jurisdictions outside the EU/EEA (such as technical support access from India) shall strictly occur on the basis of valid Chapter V transfer mechanisms, including standard EU Standard Contractual Clauses (SCCs Module 3) supplemented by robust technical measures (encryption in transit and zero local persistent storage).

7. Governing Law and Jurisdiction

This DPA is governed by the laws of Norway, with Oslo District Court (*Oslo tingrett*) as the agreed venue.