AISolutions

Data Processing Addendum (DPA)

Version 2.0 | Effective 2026-09-07 | Approved by Thore Stærk | AISolutions AS · Org. nr. 931 884 220

This Data Processing Addendum ("DPA") forms Annex A to, and is incorporated automatically into, the Customer Agreement between AISolutions AS, organisation number 931 884 220, Spannavegen 152, 5535 Haugesund, Norway ("the Processor") and the customer entity identified in that agreement ("the Controller").

Where this DPA and the Customer Agreement conflict on any matter of data protection, this DPA prevails.

1. Definitions

1.1 Terms used in this DPA that are defined in the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") carry the meaning given there. This includes "personal data", "processing", "controller", "processor", "sub-processor", "data subject", "personal data breach" and "supervisory authority".

1.2 "Services" means the cloud software provided under the Customer Agreement, comprising AidEun and SalesQuote and any associated platform components.

1.3 "Customer Personal Data" means personal data that the Processor processes on behalf of the Controller in the course of providing the Services.

1.4 "Applicable Data Protection Law" means the GDPR as incorporated into Norwegian law by the Personal Data Act (personopplysningsloven) of 15 June 2018, together with any other data protection law binding on either party.

2. Roles and Scope

2.1 The Controller determines the purposes and means of processing Customer Personal Data. The Processor processes that data only on the Controller's behalf.

2.2 This DPA governs all processing of Customer Personal Data by the Processor under the Customer Agreement. It does not apply to personal data for which AISolutions is itself the controller, such as the contact details of the Controller's representatives used to administer the commercial relationship. That processing is described in the AISolutions Privacy Policy.

2.3 Each party is responsible for its own compliance with Applicable Data Protection Law.

3. Subject Matter, Duration, Nature and Purpose

3.1 Subject matter: the provision of the Services to the Controller.

3.2 Duration: processing continues for as long as the Customer Agreement is in force, and ends when all Customer Personal Data has been deleted or returned in accordance with Section 13.

3.3 Nature of processing: collection, recording, organisation, storage, retrieval, consultation, use, transmission, restriction, erasure and destruction, carried out by automated means.

3.4 Purpose: to deliver, operate, secure, automate and support the Services in accordance with the Customer Agreement and the Controller's instructions.

3.5 The categories of data subject and types of personal data are set out in Annex I.

4. Controller Instructions

4.1 The Processor shall process Customer Personal Data only on documented instructions from the Controller, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject. In that case the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

4.2 The Customer Agreement, this DPA, and the Controller's configuration of the Services constitute the Controller's complete documented instructions at the date of this DPA. Additional instructions must be agreed in writing.

4.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Applicable Data Protection Law. The Processor may suspend performance of the instruction concerned until the Controller confirms or withdraws it.

4.4 Where the Processor processes Customer Personal Data for a purpose other than that determined by the Controller's instructions, and is not required to do so by law, it shall be considered a controller in respect of that processing and shall be responsible for its own compliance.

5. Controller Obligations and Warranties

5.1 The Controller warrants that it has a lawful basis under Article 6 GDPR, and where applicable Article 9, for the processing it instructs.

5.2 The Controller warrants that it has provided all information required by Articles 13 and 14 GDPR to the data subjects whose personal data it submits to the Services.

5.3 The Controller warrants that its instructions to the Processor comply with Applicable Data Protection Law, and that it is entitled to transfer the Customer Personal Data to the Processor for processing under this DPA.

5.4 The Controller is responsible for the accuracy, quality and legality of the Customer Personal Data it submits, and for the configuration choices it makes within the Services, including retention periods and the assignment of user access.

5.5 The Controller shall not submit to the Services any special category personal data within the meaning of Article 9 GDPR, or personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR.

6. Confidentiality

6.1 The Processor shall ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.2 Access to Customer Personal Data is limited to personnel who require it to perform the Services, and is granted on the principle of least privilege.

7. Security of Processing

7.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk to the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

7.2 The measures in place are described in Annex II. The Processor may update them provided the level of security is not reduced.

7.3 The Processor's information security management system is designed in alignment with ISO/IEC 27001. AISolutions is not currently certified to that standard; where certification is obtained, this DPA and the accompanying documentation will be updated.

8. Sub-processors

8.1 The Controller grants the Processor general written authorisation to engage sub-processors for the provision of the Services.

8.2 As at the effective date of this DPA, the Processor engages the following sub-processors:

(a) Microsoft Ireland Operations Ltd. -- Azure cloud infrastructure and Azure OpenAI Service, comprising hosting, databases, Key Vault and AI model inference. Processed and stored in Norway (Azure Norway East) and the EU. Transfer mechanism: intra-EEA processing.

(b) Microsoft Ireland Operations Ltd. -- Microsoft 365 Exchange Online, for transactional email. Processed and stored in Norway and the EU. Transfer mechanism: intra-EEA processing.

(c) Novel Teams Solutions Pvt. Ltd. -- technical lead, production support, development and engineering. Remote access only from India, with no local persistent copies. Transfer mechanism:

Standard Contractual Clauses (Module Three) together with a Transfer Impact Assessment.

The Processor maintains a current register of authorised sub-processors, including each sub-processor's location, processing purpose and transfer mechanism, and shall make it available to the Controller on request.

8.3 The Processor shall notify the Controller of any intended addition or replacement of a sub-processor at least **30 days** before that sub-processor begins processing Customer Personal Data. Notification is given by email to the Controller's registered contact.

8.4 The Controller may object to an intended change on reasonable grounds relating to data protection, in writing, within the notice period. Where the parties cannot resolve the objection, the Controller may terminate the affected part of the Services without penalty and receive a pro-rata refund of prepaid fees for the terminated period.

8.5 The Processor shall impose on each sub-processor, by written contract, data protection obligations that are no less protective than those set out in this DPA.

8.6 The Processor remains fully liable to the Controller for the performance of each sub-processor's obligations.

9. International Transfers

9.1 Customer Personal Data is hosted within the European Economic Area, in Microsoft Azure's Norway East region.

9.2 Where personal data is transferred to, or accessed from, a country outside the EEA that is not the subject of an adequacy decision, the transfer takes place on the basis of a valid Chapter V transfer mechanism. Where Standard Contractual Clauses are relied upon, these are the clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, with Module 3 (processor to processor) applying, supplemented by a documented transfer impact assessment and by supplementary technical measures including encryption in transit and the prohibition of local persistent storage.

9.3 Technical support access from India by Novel Teams Solutions Private Limited takes place on this basis. That access is remote only; no local copies of Customer Personal Data are retained.

10. Government and Law Enforcement Access

10.1 If the Processor receives a legally binding request from a public authority, including a judicial authority, for disclosure of Customer Personal Data, it shall notify the Controller of that request before disclosing anything, unless prohibited from doing so by law.

10.2 Where notification is prohibited, the Processor shall use reasonable efforts to obtain a waiver of the prohibition, and shall document the efforts made so that they can be produced to the Controller or a supervisory authority.

10.3 The Processor shall challenge any request that it assesses to be unlawful under the law of the requesting authority, or which conflicts with Applicable Data Protection Law, including by seeking interim measures where available.

10.4 Any disclosure shall be limited to the minimum amount of data reasonably necessary to respond to the request.

10.5 The Processor shall maintain a record of requests received and disclosures made, and shall make that record available to the Controller on request.

11. Assistance with Data Subject Rights

11.1 The Processor shall assist the Controller, by appropriate technical and organisational measures and insofar as this is possible, in fulfilling the Controller's obligation to respond to requests for exercising the data subject rights set out in Chapter III GDPR, including access, rectification, erasure, restriction, portability and objection.

11.2 Where the Processor receives a request directly from a data subject relating to Customer Personal Data, it shall not respond to the substance of the request but shall forward it to the Controller without undue delay.

12. Personal Data Breach, Impact Assessments and Prior Consultation

12.1 The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and in any event in sufficient time to allow the Controller to meet its own obligations under Articles 33 and 34 GDPR.

12.2 The Processor shall make an initial notification as soon as it has enough information to be useful to the Controller, rather than waiting until the position is fully established. The notification shall describe, to the extent known, 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 to address it. Where the information cannot be provided at the same time, it shall be provided in phases without undue further delay.

12.3 The Processor shall assist the Controller in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to it. This includes assistance with data protection impact assessments and with prior consultation of the supervisory authority.

13. Deletion and Return

13.1 On termination or expiry of the Customer Agreement, the Processor shall, at the Controller's choice, delete or return all Customer Personal Data, and delete existing copies, within 90 days, unless Union or Member State law requires continued storage.

13.2 The Controller may configure retention periods within the Services. The defaults are 12 months for conversation logs, configurable between 30 days and 24 months, and 24 months for RFQ records, configurable to 12, 24 or 36 months. Retention periods outside these parameters require the approval of the AISolutions Privacy Lead.

13.3 Termination of the Customer Agreement overrides any configured retention period and triggers deletion or return under Section 13.1.

13.4 The Processor shall confirm deletion in writing on the Controller's request.

13.5 Backup copies are deleted in accordance with the Processor's backup cycle, and in any event within 90 days of the deletion of the primary data. Until deletion, backup copies remain subject to this DPA.

14. Audits and Inspections

14.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. This may take the form of a description of the technical and organisational measures implemented, summaries of independent assessments where available, and responses to reasonable security questionnaires.

14.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

14.3 Audits shall be conducted on at least 30 days' written notice, during normal business hours, no more than once in any twelve-month period unless a personal data breach has occurred or a supervisory authority requires otherwise, and subject to reasonable confidentiality obligations. Each party bears its own costs.

15. Records of Processing

15.1 The Processor maintains a record of all categories of processing carried out on behalf of the Controller, in accordance with Article 30(2) GDPR, and shall make that record available to the Controller or to a supervisory authority on request.

16. Artificial Intelligence Processing

16.1 Model inference for the Services is performed using Microsoft Azure OpenAI Service, hosted within the European Economic Area.

16.2 Customer Personal Data, prompts, email content and documents submitted to that service are not used to train, fine-tune or otherwise improve any foundation model. This is assured contractually by the terms of the Azure OpenAI Service.

16.3 Prompts and inference payloads are processed transiently for the purpose of generating a response and are not retained by the model provider beyond the period necessary to return that

response, save where retention is required by the provider for abuse monitoring under terms disclosed to the Controller.

16.4 Output generated by the Services may be inaccurate. The Controller remains responsible for reviewing output before relying on it, and for any decision taken on the basis of it. Nothing in this Section limits the Controller's obligations under Article 22 GDPR in respect of automated decision-making.

17. Costs of Assistance

17.1 The assistance described in Sections 11 and 12, and the audit rights in Section 14, are provided at no additional charge to the extent that they are proportionate to the Services and to the nature of the processing.

17.2 Where a request requires effort materially beyond that level, in particular a repeated or unusually extensive audit, or assistance with a volume of data subject requests that is disproportionate to the Services, the Processor may charge its reasonable costs. The Processor shall notify the Controller of the expected cost before incurring it, and shall not withhold assistance while the cost is being agreed.

17.3 Nothing in this Section permits the Processor to make compliance with a legal obligation conditional on payment.

18. Liability

18.1 The liability of each party under this DPA is subject to the limitations and exclusions of liability set out in the Customer Agreement, save that nothing in this DPA or the Customer Agreement limits either party's liability to a data subject under Article 82 GDPR, or any liability that cannot be limited under Applicable Data Protection Law.

19. Changes to this DPA

19.1 The Processor may amend this DPA where necessary to reflect a change in Applicable Data Protection Law, a decision of a supervisory authority, a change to the Services, or a change to the Processor's sub-processors or security measures.

19.2 The Processor shall notify the Controller of any material change at least 30 days before it takes effect, by email to the Controller's registered contact and by publication of the revised DPA at https://www.aisolutions.no/dpa.

19.3 Where a material change adversely affects the Controller's rights, the Controller may object in writing within the notice period. Where the parties cannot resolve the objection, the Controller may terminate the affected part of the Services without penalty.

19.4 Continued use of the Services does not constitute acceptance of a material change to this DPA.

19.5 Each version of this DPA carries a version number and an effective date. Previous versions are retained and are available from the Processor on request.

20. Governing Law and Jurisdiction

20.1 This DPA is governed by the laws of Norway.

20.2 The courts of Norway have exclusive jurisdiction, with Oslo District Court (Oslo tingrett) as the agreed venue in the first instance.

21. Contact

Questions about this DPA, and requests under it, should be addressed to:

AISolutions AS Spannavegen 152, 5535 Haugesund, Norway Email: privacy@aisolutions.no

---

Annex I - Details of Processing

Categories of data subject

- Employees, contractors and other authorised users of the Controller
- The Controller's customers, suppliers and business contacts, where their details appear in documents, quotations or correspondence processed through the Services
- Recipients of documents and communications generated by the Services

Types of personal data

- Identification and contact data: name, job title, business email address, business telephone number
- Account data: user identifier, authentication data, role and permission assignments
- Content data: free text in prompts, emails, quotations and documents submitted to or generated by the Services, which may contain personal data determined by the Controller
- Usage and technical data: system audit logs, access logs, IP address, timestamps

Special categories of personal data

The Services are not designed for the processing of special categories of personal data within the meaning of Article 9 GDPR, or of personal data relating to criminal convictions and offences. The Controller shall not submit such data to the Services.

Frequency of processing

Continuous, for the duration of the Customer Agreement.

Retention

As set out in Section 13.

Annex II - Technical and Organisational Measures

The measures below are those implemented by the Processor at the effective date of this DPA, in accordance with Article 32 GDPR.

Pseudonymisation and encryption

- Customer Personal Data at rest is encrypted using Transparent Data Encryption on the database tier and platform-managed encryption on object storage
- Data in transit between the Controller and the Services is encrypted using TLS 1.2 or above
- Data in transit between service components within the hosting environment is encrypted

Confidentiality, integrity, availability and resilience

- Authentication is performed through Microsoft Entra ID, with multi-factor authentication required for administrative access
- Access is granted on a role-based, least-privilege basis and reviewed periodically
- Production, staging and development environments are logically separated
- Network access to service components is restricted to defined sources
- Application and platform events are logged centrally and retained for defined periods

Availability and restoration

- Databases are protected by automated point-in-time backups with a 7-day recovery window, and by long-term retention copies
- Backups are stored redundantly within the hosting region
- Restoration procedures are documented

Testing and evaluation

- Security configuration of the hosting environment is assessed against a documented baseline, and findings are recorded in a register with owners and due dates
- Dependencies are monitored for known vulnerabilities and findings are tracked to resolution
- Changes to production are subject to review before deployment

Organisational measures

- An information security management system is maintained, designed in alignment with ISO/IEC 27001
- Personnel with access to Customer Personal Data are bound by confidentiality obligations
- A documented incident response process is in place, including notification to affected controllers
- Sub-processors are subject to written contracts imposing equivalent data protection obligations

Hosting

- Microsoft Azure, Norway East region
- Model inference through Azure OpenAI Service within the European Economic Area