

DATA PROCESSING AGREEMENT (“DPA”) - NORA SOFTWARE AS

1. PROCESSOR AND CONTROLLER ROLES AND RESPONSIBILITIES

The **supplier** will in order to provide the AI based meeting assistant service, mentrai.ai, process personal data as a **processor**.

Customer will act as the **controller** when the supplier processes personal data on the customer’s behalf. Customer’s initial instructions and further processing details are set out below in sec. 4.

Terms defined in the EU General Data Protection Regulation (“**GDPR**”) art. 4 shall be applied to this DPA and understood in accordance with the GDPR definitions.

2. WARRANTY

Supplier warrants that it has implemented appropriate technical and organizational measures in such a manner that its processing of personal data under this DPA will meet the requirements of applicable data protection law and ensure the protection of the rights and freedoms of the data subjects.

If supplier fails to comply with its obligations pursuant to this DPA it shall be deemed a breach of the agreement.

3. PROCESSING DETAILS

Supplier warrants it will meet the requirements under GDPR art. 28 by:

- a) Only process personal data as instructed by the customer in the DPA or later written instruction.
- b) Notify the customer if supplier believes that an instruction is in violation of applicable data protection laws.
- c) Ensure that persons who process personal data are subject to a duty of confidentiality.
- d) Implement appropriate technical and organizational measures to ensure a level of security for personal data appropriate to the risk.
- e) Assist customer in its duty to respond to data subjects' requests to exercise their GDPR rights.
- f) Fulfill the requirement for data breach notification and assistance.
- g) Assist customer with data protection impact assessment and any cooperation with the supervisory authority.
- h) Immediately inform the customer in writing of any legal obligation that requires supplier to disclose personal data that supplier processes on behalf of the customer.
- i) Demonstrate compliance with the obligations under GDPR art. 28 by making available necessary information, on customer’s request.
- j) Allowing and contributing to any reasonable audits directed by the customer.
- k) Delete or return personal data and copies at the customer’s choice the end of the service relating to the processing.

As the potential scope of e, f, g and j above is uncertain, these tasks are subject to additional payment on a time-and-material basis according to applicable rates.

4. INITIAL INSTRUCTIONS OF PROCESSING

Purposes	<p>The purposes of the processing are the delivery of the following services or tasks by the processor to the controller:</p> <p>In order to provide the service as described on mentr.ai</p>
Categories of data	<p>The personal data processed comprises the following:</p> <p>name, email address, profile picture, employment details, job title, career information, meeting history, meeting audio</p>
Frequency of the transfer	<p><input checked="" type="checkbox"/> Continuous basis</p> <p><input type="checkbox"/> One-off</p> <p><input type="checkbox"/> Other</p>
Categories of data subjects	<p>Controller’s representatives and end users, such as employees, job applicants, contractors, collaborators, partners, customers and potential customers of the controller</p>
Processing operations (nature of processing)	<p>Storage, backup, transcription of meeting audio to text, transfer to customer CRM and ATS (if enabled by the customer)</p>
Duration of retention	<p>As decided by the data controller (customer). Meeting audio is transcribed in real-time and only stored transiently.</p>
Location of processing operations	<p>All processing of personal data is done within EU/EEA.</p> <ul style="list-style-type: none"> ● Cloudflare for hosting our website and the Mentr service ● Google for calendar and user data and Anthropic AI models ● Microsoft for calendar and user data and OpenAI data models ● Speechmatics for transcription ● Fly.io for transcription and proxying ● Convert API for file conversion <p>The Customer grants the supplier a general mandate to enter into agreements with sub-processors provided that the agreement is written and imposes the same privacy obligations as supplier has committed to. Supplier will be responsible for its own sub-processors.</p> <p>Supplier will notify the customer of any intended changes of sub-processors or locations of processing offering the customer the opportunity to object. If the customer objects to supplier’s</p>

	engagement of a sub-processor, supplier is free to terminate the agreement, and both parties are free of their obligations.
Security measures	<p>Security measures carried out:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Measures of pseudonymisation and encryption of personal data <input checked="" type="checkbox"/> Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services <input checked="" type="checkbox"/> Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident <input checked="" type="checkbox"/> Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing <input checked="" type="checkbox"/> Measures for user identification and authorisation <input checked="" type="checkbox"/> Measures for the protection of data during transmission <input checked="" type="checkbox"/> Measures for the protection of data during storage <input checked="" type="checkbox"/> Measures for ensuring physical security of locations at which personal data are processed <input checked="" type="checkbox"/> Measures for ensuring events logging <input checked="" type="checkbox"/> Measures for ensuring system configuration, including default configuration <input checked="" type="checkbox"/> Measures for internal IT and IT security governance and management <input checked="" type="checkbox"/> Measures for ensuring data minimisation <input checked="" type="checkbox"/> Measures for ensuring data quality <input checked="" type="checkbox"/> Measures for ensuring limited data retention <input checked="" type="checkbox"/> Measures for ensuring accountability <input checked="" type="checkbox"/> Measures for allowing data portability and ensuring erasure

5. MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

Supplier shall

- a) implement the technical and organizational measures checked off for in sec. 4 to ensure the security of the personal data, and
- b) ensure that the level of protection of data subject guaranteed by applicable data protection law including the GDPR is not undermined.