Noteless

Data Processing Agreement

1 About the agreement

This data processing agreement with appendices (hereinafter referred to as the "**Data Processing Agreement**") regulates the rights and obligations between the data controller ("**Controller**") and Noteless ("**Processor**") (hereinafter referred to as the "**Parties**") have under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (hereinafter referred to as "**GDPR"**) and any other adjacent and relevant national legal obligations applicable to the Parties ("**Applicable Privacy Law**"). National Guidelines, such as the Standard for Information Security and Privacy in the Norwegian Health Care Sector (Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 7.0 - Helsedirektoratet, hereinafter the "**Standard**") applies insofar as this is required by the Controller.

- The Data Processing Agreement relates to the provision of Noteless services under the description, rights and obligations provided in the agreement executed by the Parties for the provision of Processor commercial services to the Controller (the "**Agreement**"). The description of the processing of personal data is described in Appendix 1.

In the event of a conflict or divergence between the provisions of the Data Processing Agreement and the Applicable Privacy Law, the provisions of the Data Processing Agreement shall prevail regarding what is allowed by law to be agreed by the involved Parties. In the event of a conflict between the Data Processing Agreement and the Agreement, the Data Processing Agreement shall apply.

Attachment to the agreement:

- Appendix 1: Purpose of processing, data and processing operations
- Appendix 2: Information security measures
- Appendix 3: Subcontractors

2 Purpose of the agreement

The purpose of the Data Processing Agreement is to ensure that the processing of personal data that is necessary to fulfill the purpose of the Agreement occurs in accordance with the requirements of GDPR Article 28.

3 Definitions

The terms "personal data", "health data", "processing", "controller" and "data manager", "data processor", "personal data breach," and "health data" shall be understood as defined in the GDPR.

4 Scope of the data processing agreement

This Data Processing Agreement applies to all processing of personal data carried out by the Processor on behalf of the Controller to comply with the obligations provided in the Agreement.

This Data Processing Agreement will also apply to further processing of personal data based on any written agreements between the parties that are entered into during the term of the Data Processing Agreement and which may involve the Processor processing personal data on behalf of the Controller (hereinafter referred to as "**Subsequent Written Agreements**").

5 Purpose of processing, data and processing operations

The purpose and duration of the processing of personal data, what personal data is processed, categories of data subjects, and processing activities are set out in Appendix 1.

6 The framework for the processing of health and personal data

The Controller shall at all times have full control over the personal data processed by the Processor under this Data Processing Agreement. Unless otherwise agreed or required by the Applicable Privacy Law, the Controller has the right to access and inspect the personal data processed by the Processor.

7 Obligations of the Controller

The Controller has the right and obligation to determine the purposes of the processing and the means of implementation, which is established in Appendix 1.

The Controller shall comply with the obligations that follow from the data protection regulations, according to Article 24 of the GDPR, relevant health legislation and other special legislation, as well as this Data Processing Agreement.

The Controller is responsible for ensuring that the data protection principles are complied with, in accordance with Article 5 of the GDPR, and shall ensure that the processing of personal data is based on a valid legal basis.

The Controller shall notify the Processor in writing of any legal requirements and other requirements relevant to the Processing, including requirements identified by the Processor as relevant, regardless of whether such requirements form part of Applicable Privacy Law. The Controller shall clearly describe what is required from the Processor to meet such requirements and shall provide documented instructions describing how the Processing shall be performed in order to comply with them.

8 Obligations of the Processor

The Processor must:

a) only process personal data in accordance with the Controller's documented instructions as set out in this Data Processing Agreement. The Processor shall only process the personal data in the manner and to the extent necessary to achieve the purpose of the Agreement as described in Appendix 1. Personal data to which the the Processor has access as a result of the Agreement may not be used for the Processor's own purposes or other purposes in the Processor's interest, except as expressly provided in this Data Processing Agreement or the Agreement.

b) upon request, assist the Controller in fulfilling the Controller's obligation to respond to requests from data subjects pursuant to Chapter 3 of the GDPR and notify the Controller without undue delay of requests from the data subject.

c) assist the Controller in ensuring compliance with Articles 32 to 36 of the GDPR, considering the nature of the processing and the information available to the Processor.

d) make available to the Controller all information necessary to demonstrate compliance with the Parties' obligations under Articles 28 and 32 of the GDPR and facilitate and contribute to audits and inspections carried out under the auspices of the Controller or supervisory authorities.

e) The Processor shall notify the Controller in writing of any personal data security breaches. The notification shall contain information enabling the Controller to fulfill its obligations under Articles 33 and 34 of the GDPR, provided that the Processor has such information. The notification shall be given without undue delay after the Processor became aware of the breach. If it is not possible for the Processor to provide all relevant information at once, the information may be provided in stages without undue delay.

If instructions as mentioned in a) above entail additional costs to the Processor (at Processor's own evaluation), the Processor shall give notice of this to the Controller, and the Parties shall agree on any additional payment.

Assistance as mentioned in c) and d) above will be provided at the hourly rates agreed between the parties or, if not agreed, at the Processor's current hourly rates.

In no event the Processor shall be required to provide the additional services in a), c), and d) in the case that the Controller does not agree with the additional payments as provided in the two paragraphs above.

The Processor shall notify the Controller in writing as soon as possible if it has reasonable grounds to believe that (i) an instruction from the Controller may result in the Processor being in breach of applicable Applicable Privacy Law, or (ii) applicable law in the EEA requires the Processor to process personal data beyond the scope of the Controller's documented instructions, unless such Applicable Privacy Law prohibits such notification.

9 Safety and Security

The Processor shall implement appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The Processor shall, as a minimum, implement the measures required under Article 32 of the GDPR and in accordance with the recommendations set out in the Standard.

The Processor's current security measures are described in Appendix 2. The Processor may change its security measures on an ongoing basis, provided that the changes do not undermine the overall level of security described in Appendix 2. In the event of changes that affect the agreed security level, these shall be notified to the Controller and documented as amendments to the Data Processing Agreement.

10 Duty of Confidentiality

The Processor's employees and others acting on the Processor's behalf in connection with the processing of personal data in accordance with this Data Processing Agreement, the Agreement and Subsequent Written Agreements between the parties shall be subject to a duty of confidentiality in accordance with this Data Processing Agreement and Applicable Privacy Law.

Persons who are authorized to process personal data undertake to treat the data confidentially. The same applies to any subcontractors or Sub-processors.

Employees and others acting on behalf of the Processor in connection with the processing of personal data must have signed a declaration of confidentiality. The provision applies correspondingly to subcontractors or Sub-processors.

The Processor shall ensure that everyone who processes personal data under the Agreement is familiar with the duty of confidentiality.

In addition, the parties have a duty of confidentiality regarding confidential information related to each other's business that is communicated in connection with the assignment.

The parties are obliged to take the necessary precautions to ensure that material or information is not made known to others in violation of this section.

The duty of confidentiality also applies after the termination of the Agreement.

11 Use of Subcontractors

The Controller grants the Processor a general authorization to engage other processors ("**Sub-processors**") to perform tasks under this Data Processing Agreement, provided that agreements are entered into in accordance with Article 28(4) of the GDPR. The Processor shall be fully liable to the Controller for the Sub-Processor fulfilling its obligations.

An overview of Sub-processors used as part of the Processor's services can be found in Appendix 3

The Processor shall notify the Controller of any plans to use new Sub-processors or to replace Sub-processors, thereby giving the Controller the opportunity to object to such changes. If the Controller has not objected to the change within 30 days of such notice, it shall be deemed to have accepted the change. If the Controller objects to the change within the time limit, and the Processor cannot reasonably continue the processing without implementing the change, the Controller has the right to terminate the Agreement, including this Data Processing Agreement, with 30 days' notice.

12 Transfer to a third country

The Processor shall not transfer personal data to a third country or an international organization, including through the engagement of Sub-processors, unless such transfer is (i) carried out on documented instructions from the Controller or (ii) necessary due to the Processor’s use of Sub-processors located in third countries for which the European Commission has issued an adequacy decision in accordance with Article 45 GDPR.

Any transfer of personal data to third countries shall take place in accordance with the requirements of Chapter V of the GDPR. Where the Processor engages a Sub-processors located in a third country that benefits from an adequacy decision, such transfer shall be deemed to comply with the Controller’s instructions, provided that the Processor has informed the Controller of the relevant Sub-processors in accordance with this Agreement.

13 Limitation of Liability

The Parties' liability for damages that affect the data subject or other natural persons and that are due to a breach of the Applicable Privacy Law, shall follow the provisions of Article 82 of the GDPR.

Any limitation of liability in the Agreement also applies to liability arising from Article 82 of the GDPR.

The Parties are each liable for any infringement fees imposed to each of them pursuant to Article 83 of the GDPR.

14 Auditing

The Processor shall make available to the Controller information necessary to demonstrate compliance with this Data Processing Agreement and the Personal Data Act.

Upon request, the Controller may be provided with any data protection audit reports prepared by third parties on behalf of the Processor. The Controller shall have the right to present such audit reports to its external auditors and to supervisory authorities.

Upon request, the Controller, through an auditor or similar third party subject to confidentiality obligations, has the right to conduct audits of the Processor. The Processor shall also enable and contribute to audits by supervisory authorities. Requests for audits shall be given with at least 14 days' notice. Audits may not be carried out more than once a year, unless required by Personal Data Act.

If an audit reveals breaches of this Data Processing Agreement or the Personal Data Act, the Processor shall correct such breaches within a reasonable time.

Each party covers its own costs associated with an audit.

15 Duration and termination

This Data Processing Agreement applies for as long as the Processor processes personal data on behalf of the Controller in connection with the Agreement.

The Controller has the right to terminate the Agreement with future effect if the Processor breaches its obligations in this Data Processing Agreement or obligations related to the role as data processor under the GDPR.

Upon termination of the Data Processing Agreement, the Processor shall, if the Controller requests, delete all personal data and confirm to the Controller that it has done so. Termination of the Data Processing Agreement has the effect of terminating the Agreement.

The Data Processor's obligations upon termination of the agreement are described in more detail in Appendix 1.

Appendix 1

Description of the purpose, scope and duration of the processing

Purpose of the treatment:

Processor will process personal data to the extent necessary to achieve the purpose of the Agreement. The processing involves the Processor transcribing the conversation that the User (as defined in the Agreement) wants transcribed into a written note, that the User can edit, copy and move to other information systems such as a patient record, and aggregate information for documentation draft, suggestions, and evaluations, if part of the Services under the Agreement, the tools intended to support the Controller in taking decisions and draft documents. The purpose of the processing is to streamline and quality-assure the User's note-taking and help the User to focus his or her attention on the interlocutor without writing down what is being said during the conversation, and to support the decision-making process of the Controller and assist with document drafting.

Processing Activities:

- Transcribing involves a series of processing activities.
- Conversion of audio to text: Transcription is activated at the start of the call. Processor transmits the captured audio to software that uses AI technology to convert audio to text.
- Anonymization of text: Text originating from consultations and dictations is processed through an AI-based filtering tool that removes information that typically identifies individuals, ensuring the resulting text cannot be directly linked to specific persons. For uploaded documentation and pasted text, anonymization is limited to personal identification numbers.
- Conversion of anonymized text into a medical note: The conversation is converted into a structured note that can be copied into other professional systems and edited by the User.
- Submission of text and information to AI technology to provide outputs related to decision making support, including document drafting, referral information, summary of patient information, evaluations, and suggestions.

Categories of data subjects:

Individuals participating in the conversation being transcribed, as well as any identifiable third parties mentioned in the conversation.

Categories of personal data:

Name and health information that appears in the call or provided by the Controller in another manner, including the User's assessments and recommendations.

Special categories of data: health data and possibly other data defined as special categories of data in Article 9 of the GDPR if such data is included in the call.

The scope of personal data:

The scope of information corresponds to health information from the number of consultations per user per day.

Duration of the processing:

The processing shall take place for as long as the Processor processes personal data on behalf of the Controller in connection with the Agreement.

Deletion of personal data:

- Generated notes and drafts are automatically deleted once a day and it is assumed that information has been transferred to other professional systems in accordance with the User's documentation obligation.
- All documentation and personal data are deleted within 24 hours.
- As the personal data is deleted, the Processor shall refer to the Controller in the event of inquiries from the data subject regarding access, correction or deletion of information.
- The Controller is solely responsible for the further processing of the personal data possibly transferred to other systems and patient records.
- Before AI processing of transcriptions, direct personal identifiers that aren't strictly necessary for the service to function, such as personal identification numbers and phone numbers, are anonymized.

Termination of the agreement:

Upon termination of the Data Processing Agreement, the Processor shall delete any personal data processed on behalf of the Controller, unless retention is required by applicable law. As part of the Processor's standard system design, patient transcripts, notes, and similar consultation data are automatically deleted within 24 hours of creation.

Appendix 2

Information security measures

The following information security requirements have been agreed in addition to the provisions in section 9 of the Data Processing Agreement

No.	Theme	Requirements/description
1.	Standard for information security in the health and care sector	The Processor must satisfy relevant requirements in the Standard
	Management system/procedures for the processing of personal data	The Processor has an information security management system that ensures that the data processor in a systematic and documented manner implements and maintains appropriate information security in the business in line with relevant requirements and within acceptable risk.
	Safety audit	The Processor shall regularly conduct internal audits of information security. The documentation shall be available to the Controller.
	Securing data	Customer Data (As defined in the Agreement) is encrypted during transportation and storage to ensure integrity and confidentiality. Customer Data is stored separately from other users' data. Patient transcripts, notes, and related consultation data are automatically deleted within 24 hours of creation as part of the Processor's standard system design
	Access management	All access and interactions by the Processor shall be logged. Access shall be limited to what is necessary to provide the services. For users with privileged access, irrespective of whether this provides direct access to the Controller's data, each user shall be personalized, strictly limited and controlled, and with associated necessary security measures.
	Authentication	Any access and use by the Processor requires login and authentication using an adequate and appropriate multi-factor authentication solution.
	Measures against digital attacks	The Processor has implemented safeguards to protect against cyberattacks, including denial-of-service attacks and malicious code. The Processor uses advanced monitoring systems to continuously detect and promptly investigate unusual or suspicious activity that could indicate a security incident.

	Logging and traceability	The Processor shall implement logging that shows access to the Controller's data if such access is relevant. The logs shall be secured against unauthorized access, modification and deletion.
	Accessibility	The Processor must have an infrastructure that ensures capacity and availability in line with the agreed service level.
	Data	The Controller's data shall not be used for testing purposes unless agreed in writing with the Controller. Any anonymization shall take place on the instructions of the Controller. In cases where the Controller's data is used for testing by agreement, it shall be secured in the same way as production data. Where production data is used for testing purposes, it shall be deleted after testing has been completed.
	Deletion and return	Generated notes are automatically deleted after 24 hours. The Processor shall have routines and technical solutions to ensure that all Controller data is deleted or returned upon instruction from the Controller, or upon termination of the Data Processing Agreement. This also includes data stored on backup media and logs.
	Storage time	The Processor stores the Controller's data temporarily and for no longer than 24 hours after the transcription took place.
	Backup and restore	The Processor shall have sound backup and restoration routines that are tested regularly.
	Encryption when storing	Data is encrypted when stored and identifying characteristics are removed from generated notes that are temporarily stored at the Processor.
	Encryption in communication	Data must always be encrypted in communication in accordance with NSM specifications.
	Access control	The Processor shall have adequate physical security where the Controller's data is accessible.
	Security architecture	The Processor must separate data belonging to different customers. The Processor's own data shall be separated from the customers' data. The Processor shall have procedures in place to ensure that the Controller's data is not transferred to other companies unless this has been agreed in writing with the Controller.
	Authorization register - if applicable.	The Processor shall at all times maintain an updated authorization register for personnel authorized to access the Controller's information and services.

Appendix 3

The Controller expressly provides the Processor with a general written authorization to engage with Sub-processors.

A list of the Sub-processors used by the Processor at any given time is available at trust.noteless.com.

In the event that the Controller objects to the use of any given Sub-processor, the Parties shall discuss in good faith its continued use.