DATA PROCESSING AGREEMENT

In accordance with the EU General Data Protection Regulation 2016/679

between

COMPANY NAME

Org. no: NO 000 000 000
Controller

and

CONFRERE AS

Org. no: NO 918 544 178
Processor

Dated: July 22, 2020

1. About the agreement

This data processing agreement (hereinafter “the Agreement”) regulates rights and obligations between the Controller and the Processor (hereinafter “the parties”) pursuant to:

- 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 (hereinafter “the General Data Protection Regulation”);

- Any law, implementing regulations or other regulations which amends or repeal/replace the above.

In the event of conflict between the provisions of the Agreement and the framework that follows from data protection legislation or other relevant health legislation, the provisions of the Agreement shall cede precedence.

2. Definitions

The terms “personal data”, “processing”, “controller”, “processor”, “personal data breach” and “personal health data” shall be understood as they are defined in Article 4 of the General Data Protection Regulation as applicable.

“Breach”: breach of data security and use of an information system in violation of established routines. The use of an information system that is not in accordance with instructions from the Controller or applicable data protection legislation shall be considered a breach.

3. Background and purpose of the Agreement

This Agreement is entered into between the parties and outlines the conditions generally applicable to the processing of personal health data and personal data which the Processor carries out on behalf of the Controller.

The purpose of the Agreement is to safeguard the processing of personal health data and personal data on behalf of the Controller, so that personal health data and personal data is not used improperly or disclosed to unauthorised persons.

4. Scope

This Agreement shall apply to all processing of personal health data and personal data which the Processor carries out on the basis of the Terms of Service. In the event of conflict between this Agreement and the Terms of Service, this Agreement shall take precedence. Services that are covered by this Agreement are the services which are covered by the Terms of Service and which entail the processing of personal health data and personal data.

This Agreement shall also apply to other processing of personal health data and personal data based on any written agreements between the parties which are entered into during the effective period of this Agreement and which entail the Processor processing personal health data and personal data on behalf of the Controller (hereinafter “Subsequent Written Agreements Between Parties").

Personal data shall only be used for the purposes that follow from this Agreement, the Terms of Service and Subsequent Written Agreements Between Parties insofar as strictly necessary in order to implement and fulfil the requirements in the agreements.

5. Purpose of the processing, data and processing activities

The purpose and duration of the processing of personal health data and personal data, which personal health data and personal data that are processed, categories of data subjects and the nature of the processing are set out in Appendix 1.

A more detailed description of the processing, the purpose of the processing and which personal health data and personal data that are covered is given in the Terms of Service and Subsequent Written Agreements Between Parties (if applicable).

6. Framework for the processing of personal health data and personal data

The Controller shall at all times have full beneficial rights over the personal health data and personal data that the Processor are authorised to process under this Agreement. The Processor does not have any independent right of benefit with regard to the personal health data and personal data and cannot process such data for its own purposes.

The Controller has, unless otherwise agreed or follows from laws, the right of access to and access in the personal health data and personal data processed by the Processor.

7. The Controller's obligations

The Controller shall fulfil the obligations that are stipulated in the General Data Protection Regulation, relevant health legislation and other special legislation, as well as this Agreement.

8. The Processor's obligations

8.1. General

The Processor undertakes to process personal health data and personal data merely in accordance with all applicable laws and regulations, this Agreement, the Terms of Service, the Controller's documented instructions and other applicable agreements between the parties, as well as the "Code of conduct for information security in the healthcare and care services". The Processor shall not, by any act or omission, place the Controller in a situation that the Controller breaches any provision in any applicable law or regulation.

The Processor shall not:

a. process personal health data and personal data for any purposes or to any greater extent other than as follows from this Agreement, the Terms of Service and any Subsequent Written Agreements Between Parties;

b. process personal health data and personal data beyond what is necessary in order to fulfil the Processor's obligations in accordance with the agreements applicable at any time;

c. disclose, hand over or transfer personal health data and personal data in any form on its own initiative except by prior agreement with the Controller or the Controller has consented to this in writing;

d. collect or transfer personal health data and personal data from/to a third party;

e. process personal health data and personal data they gain or have access to by the assignment from the Controller in any manner other than as stipulated in this Agreement, the Terms of

Service and any Subsequent Written Agreements Between Parties.

The Processor shall:

a. maintain ongoing control over all categories of processing activities carried out on behalf of the Controller;

b. give the Controller access to and access in personal health data and personal data processed by the Processor;

c. establish and maintain an overview of all data and processing or, where relevant, a record of its own processing activities in accordance with Article 30 of the General Data Protection Regulation;

d. take all reasonable measures to ensure that personal health data and personal data is accurate and updated at all time;

e. establish routines to erase information which is no longer needed based on the purpose of the processing and erase information in accordance with established routines and guidelines;

f. have routines and technical ability to restrict the processing of data subjects' personal health data and personal data if the data subject so wishes in accordance with applicable legislation;

g. ensure that all persons who are given access to personal data processed on behalf of the Controller are familiar with this Agreement and applicable agreements between the parties, and are subject to the provisions of these agreements;

h. ensure that requirement of data protection by design and by default is fulfilled in the Processor's solutions. This includes building in functionality to fulfil data protection principles as well as functionality to safeguard the rights of the data subject;

i. provide the Controller with the necessary assistance so that the Controller can fulfil its obligations with respect to data subjects;

j. collaborate with and assist the Controller in connection with the fulfilment of the data subjects' rights related to data access, including responding to requests from data subjects with the aim of exercising their rights as set out in Chapter III of the General Data Protection Regulation;

k. immediately notify the Controller if the Processor believes that any instruction is in breach of the General Data Protection Regulation or other provisions concerning the protection of personal data;

l. assist the Controller in ensuring compliance with the obligations of Articles 35-36 of the General Data Protection Regulation, which concern the data protection impact assessment and prior consultation with the Norwegian Data Protection Authority (Datatilsynet).

8.2. Technical, organisational and security measures

The Processor undertakes to identify and implement all necessary and adequate planned and systematic technical, organisational and security measures to ensure there is satisfactory information security at any time in connection with the processing of personal health data and personal data.

The Processor shall:

a. establish and comply with all necessary technical and organisational measures considering continued confidentiality, integrity, accessibility and robustness in the processing of personal health data and personal data to ensure satisfactory information security in accordance with the provisions of the data protection legislation, including the requirements under Article 32 of the General Data Protection Regulation, and applicable health legislation. This encompasses among other things, insofar as is relevant, necessary measures to prevent the random or unlawful erasure or loss of data, unauthorised access to or distribution of data as well as any other use of personal health data and personal data which is not in accordance with this Agreement, and measures to restore availability and access to the data in the event of incidents;

b. have good and appropriate internal control routines;

c. have routines for authorisation and control which ensure that only the Processor's employees who have a genuine need for access to systems and data in order to perform necessary tasks for the fulfilment of the Terms of Service are able to gain such access. The level of access shall be in accordance with genuine need associated with implementation of the assignment;

d. establish necessary systems and routines to safeguard information security and follow up breaches, which shall consist of amongst other routines for reporting breaches, restoring normal status, eliminating the cause of breaches and preventing reoccurrence. Upon request, the Processor shall give the Controller access to relevant security documentation and the systems that are used to process personal health data and personal data;

e. detect, register, report and close breaches linked to information security, including logging and documenting any attempts of unauthorised access and other breaches of information security in the data systems. Such documentation shall be retained by the Processor;

f. in the event of suspected or confirmed breaches, immediately notify the Controller. In the notification shall be described the breach with an explanation of the cause, the period and the time at which the breach was discovered, the categories and approximate number of data subjects affected, the categories and approximate number of personal data records affected, the name and contact details of the data protection officer or other contact point where more information can be obtained, the estimated impact of the breach and which immediate measures have been instigated or are being considered for instigation in order to deal with the breach;

g. document any breach, including the factual circumstances associated to the breach, its impact and any remedial measures that have been implemented;

h. immediately notify the Controller in the event of the unauthorised disclosure of personal data;

i. register all authorised and unauthorised access to information. All look-ups performed shall be registered so that they can be traced to the individual user concerned (i.e. an employee of the Processor, a subcontractor or the Controller). The logs shall be retained until it is no longer considered to be of any use for them or as stipulated by the Terms of Service;

j. help the Controller to ensure fulfilment of the obligations in Articles 32-34 of the General Data Protection Regulation, i.e.:

k. security of processing;

l. notification of a personal data breach to the supervisory authority;

m. communication of a personal data breach to the data subject;

n. in connection with a security audit conducted by the Controller or a third party appointed by the Controller, present internal audit reports, internal procedures, routines, security architecture, risk and vulnerability analyses with measures and other documents of importance to the audit;

o. notify the Controller of all circumstances that lead to a change in the risk profile;

p. obtain approval from the Controller prior to carrying out any changes in the data processing at the Processor that have or can have impact on information security.

More detailed requirements concerning the Processor's information security are presented in Appendix 2 (if applicable).

In the event of breach of this Agreement or the provisions of the data protection legislation, health legislation or other relevant legislation, the Controller may demand changes in the method of processing or require the Processor to cease all further processing of data with immediate effect.

The Processor shall document its routines and all measures taken to fulfil the requirements set forth above. This documentation shall be made available to the Controller upon request.

9. Use of subcontractors

The Controller permits the Processor to use subcontractors for the fulfilment the obligations under this Agreement. The Processor uses subcontractors as specified in Appendix 3 for the services specified therein and confirms that there are no other subcontractors used.

The Processor shall:

a. ensure that the subcontractor undertakes similar obligations as the Processor under the Agreement and applicable legislation;

b. ensure that subcontractors only process personal data in accordance with this Agreement and not to a greater extent than is necessary in order to deliver the relevant service provided by the subcontractor;

c. maintain an updated list of the identity and location of subcontractors as specified in Appendix 3. The updated list shall be available to the Controller;

d. conduct a risk assessment concerning the use of subcontractors and its significance for the service before entering into an agreement with subcontractors and on the Controller request, share the assessment with the Controller;

e. at the Controller's request, present a copy of the agreement(s) that have been entered into with the subcontractors (with the exception of commercial conditions). Such agreements must at the latest be concluded before the subcontractors commence the processing of personal health data and personal data;

f. notify the Controller of any plans to use other subcontractors or change subcontractors. Such change must be notified in good time so that the Controller is given the opportunity to object

to the change. When changing a subcontractor, Appendix 3 shall be updated and sent to the Controller's contact person;

g. ensure that the Controller and the supervisory authority have the same right to access and control in respect to the processing of personal data at a subcontractor as the Controller has with respect to the Processor under Article 12 of the Agreement;

h. upon termination of the Agreement, ensure that subcontractors fulfil their obligation to erase or appropriately destroy all personal health data and personal data and any and all copies of the data as stipulated in Article 13 of the Agreement in the same manner as the Processor insofar as this does not in conflict with other statutory provisions.

The Processor shall at all time be fully responsible to the Controller for all work performed by subcontractors and for subcontractors' compliance with the provisions of this Agreement.

Access to personal health data and personal data for third parties demands a specific agreement between the parties beyond this Agreement for all other than the Processor's subcontractors.

10. Transfer of personal data to other countries

The parties to this Agreement agree that none of the personal health data or personal data processed under this Agreement shall be transferred out of Norway, unless it is specifically agreed between the parties. Moreover, archival documents with personal health data and personal data shall be placed on servers in the EU, and any exception to this shall be explicitly approved by the Controller before the processing commences.

The Processor confirms that none of the subcontractors transfer personal health data or personal data that is covered by this Agreement to other countries, with the exception of such transfers presented in Appendix 3. This also encompasses remote access from other countries.

The use of subcontractors who transfer personal health data and personal data to countries outside the EU/EEA (third countries) shall be agreed in writing with the Controller in advance. When transferring personal health data and personal data to countries outside the EU/EEA (third countries), the Processor shall use approved EU transfer mechanisms.

When transferring to other countries, regardless of whether the country is within the EU/EEA or outside the EU/EEA (third countries), the Processor shall provide necessary documentation concerning security, risk and compliance level associated with the relevant subcontractors so that the Controller receives the necessary information to be able conduct a specific risk assessment. The Controller can refuse to consent to the particular transfer based on specific risks identified through the Controller's own risk assessment.

11. Duty of confidentiality

The Processor's employees and other parties acting on behalf of the Processor in connection with the processing of personal data in accordance with this Agreement, the Terms of Service and Subsequent Written Agreements Between Parties (hereinafter "persons authorised to process personal data") are subject to a duty of confidentiality after this Agreement and applicable regulations. Persons authorised to process personal data undertake to process the data confidentially. The same applies to any subcontractors.

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

Employees and others acting on behalf of the Processor in connection with the processing of personal data shall have signed a confidentiality declaration. This provision applies correspondingly to subcontractors.

The parties in addition have a duty of confidentiality concerning confidential information rlating to each other's activities which are disclosed in connection with the assignment.

The parties are obliged to take the precautions that are necessary to ensure that data materials or information are not disclosed to others in violation of this article.

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

12. Access, verification and audit

The Controller can at any time demand access to and verification of the Processor's processing of personal data belonging to the Controller, including access to and verification of documentation for compliance with information security requirements and the Processor's internal control system.

The right of access applies to all technical, organisational and administrative matters that are relevant to the security of processing carried out by the Processor on behalf of the Controller, and other rights of access set out in law. If the Controller requests access, general information from the audit shall be made available to other controllers using the same service from the Processor.

The Controller shall insofar as possible give the Processor notice in reasonable time when requiring access and control, normally at least 30 days. For request for access to documents at least 14 days' notice should be given. The Controller shall help to ensure that access and audit can be coordinated between several controllers who receive services from the Processor. Access and audit may be carried out by the Controller or a third party appointed by the Controller. The Processor can claim reimbursement for documented additional costs incurred in such audits.

The Processor shall give the Norwegian Data Protection Authority and other relevant supervisory authorities access to and access in the processing of personal health data and personal data as follows from relevant legislation.

The Processor shall correct any breaches without undue delay. Breaches attributed to the Processor or his subcontractors shall be corrected at no cost to the Controller. The Processor shall prepare a written account of corrective measures and plan for implementation.

13. Duration and termination

This Agreement applies from when it is signed by the parties and continues to apply until the Agreement and all applicable agreements between the parties, which entail the Processor shall process personal health data and personal data on behalf of the Controller, cease to apply.

Upon termination of the Agreement, the Processor shall facilitate and assist in the return of all data that the Processor has received and processed on behalf of the Controller. The parties shall further agree how the transfer shall take place.

After all the data has been transferred to the Controller and receipt confirmed by the Controller, the Processor shall irreversibly erase or appropriately destroy all the data and any and all copies and back-ups of the data in their systems, unless mandatory statutory provisions require the personal health data and personal data continued to be stored.

If shared infrastructure is used where direct erasure is not directly possible, the Processor shall ensure that data is rendered unavailable until such data is overwritten by the system.

The Processor shall give the Controller written confirmation that the data has been transferred and erased as specified above.

14. Amendments to the Agreement

In the event of changes in applicable legislation, final rulings that give a different interpretation of applicable law, or changes in services in the Terms of Service which require amendments to this Agreement, the parties shall cooperate to update the Agreement accordingly.

15. Communication

Messages, notifications, reports and other communication between the Controller and the Processor shall take place in writing or be confirmed in writing to:

Controller	Processor
Company Name	Confrere AS Dovresvingen 6B, 1184 Oslo, Norway
Name: Example Name Role: COO	Name: Svein Yngvar Willassen Role: CEO E-mail: svein@confrere.com Mobile no.: +47 924 49 678

16. Governing law and venue

The Agreement is subject to Norwegian law and the parties accept Oslo District Court (Oslo tingrett) as the legal venue. This also applies after termination of the Agreement.

17. Signatures

This Agreement is available in two originals, whereby each party holds one original.

Controller	Processor

Controller	Processor
The document was signed digitally	*The document was signed digitally*
Name: Example Name	Name: Svein Yngvar Willassen

APPENDIX 1 — PURPOSE OF THE PROCESSING, DATA AND PROCESSING ACTIVITIES

The tables are updated on an ongoing basis.

A. Purpose and duration of the processing

The purpose and duration of the processing of personal health data and personal data is:

Name of service	Purpose of the processing	Duration of the processing
Confrere	Conduct encrypted video meetings between a professional and a client	Until the purpose has been achieved

B. Processing of personal health data and personal data

The following processing is covered by the Agreement:

Processing	Processing activities
Collection	Collection of information provided by patient or client. Collection of information provided by health care provider or professional.

Processing	Processing activities
Storage	Storage of information provided by patient or client. Retention period specified by professional. Storage of information provided by health care provider or professional. Retention period specified by professional.

C. Data types

The following personal health data and personal data are processed:

Personal data	Health data
Name Telephone number Personal identification number Payment details Email address	Time of call Duration of call Call participants

D. Categories of data subjects

The following are categories of persons whose data is processed (data subjects):

Categories of data subjects			
Health care providers	Patients	Professionals	Clients

APPENDIX 2 — DETAILED REQUIREMENTS FOR INFORMATION SECURITY

No	Topic	Requirement

No	Topic	Requirement
1.	Code of conduct for information security in the healthcare and care sector	The Processor shall comply with all relevant requirements in the Code of conduct for information security (see fact sheet 6b, and the requirements that are specified for the processor)

APPENDIX 3 — Subcontractors

The tables are updated on an ongoing basis.

Name of subcontractor	Delivery area	Location
Amazon web services	Data centre, hosting	Dublin, Ireland, Europe
Sinch AB	Sending SMS to users in the EU	Stockholm, Sweden, EU