Joint Data Controllership Arrangement

1 Joint Controllership

This arrangement is entered into by and between the organisation registered as user of the Opticloud Platform (hereafter referred to as "Data controller 1") and Fremco A/S, company registration number 30 81 54 16, Ellehammersvej 14, 9900 Frederikshavn (hereafter referred to as "Data controller 2") and sets out the division of responsibilities between Data controller 1 and Data controller 2 in relation to the processing of personal data in the context the Opticloud platform.

For the purpose of this arrangement, Data controller 1 and Data controller 2 are each a "Party" and collectively the "Parties.

1.1 According to Article 26 of the General Data Protection Regulation, joint Data controllership exists when two or more Data controllers jointly determine the purposes and means of the processing.

In the case of joint Data controllership, the joint Data controllers shall determine in a transparent manner their respective responsibilities for compliance with the obligations under the General Data protection Regulation, in particular to exercise the data subject's rights and their respective obligations to provide the information referred to in Articles 13 and 14, by means of an arrangement between them, unless and to the extent that the respective responsibilities of the Data controllers are laid down in Union or Member States' national law to which the Data controllers are subject.

The arrangement shall, in accordance with Article 26(2) of the General Data Protection Regulation, duly reflect the respective roles of the joint data controllers and their relationship with the data subjects. The main content of the arrangement must also be made available to data subjects.

However, regardless of the terms of the arrangement, the data subject may exercise their rights under the General Data Protection Regulation with regard to and against the individual data controller.

Similarly, the "internal" division of responsibilities in the joint data controller arrangement does not prevent the supervisory authority from exercising its powers in relation to any of the data controllers.

1.2 Data controller 1 and Data controller 2 agree that they are joint data controllers in the context of processing of information logged by equipment manufactured by Data Controller 2 and operated by Data Controller 1 (or anyone assigned by Data Controller 1 to operate the equipment). In assessing this, account has been taken, inter alia, to the following factual circumstances:

- Data controller 1 is operating equipment for fiber blowing, manufactured by Data controller 2.
- The equipment is logging technical data along with the identity of the operator and the GPS position of the equipment and storing this information in the Opticloud solution.
- Both parties have interests in the logging and storage of the information in question for documentation and analysis purposes

1.3 This arrangement is designed to enable Data controller 1 and Data controller 2 to comply with the joint liability requirements of Article 26 of the General Data Protection Regulation. The arrangement sets out the respective responsibilities of Data controller 1 and Data controller 2 to comply with the obligations of the General Data protection Regulation, in particular to exercise the data subject's rights and the obligation to provide the information referred to in Articles 13 and 14.

1.4 With respect to all processing activities not defined in clause 2.2 below, each Party is an independent controller within the meaning of Article 4 No. 7 of the General Data Protection Regulation.

2 Overall allocation of responsibilities

2.1 Each Party acknowledges and confirms that they will observe all applicable requirements of data protection laws including the General Data Protection Regulation, particularly with regard to the lawfulness of the joint processing operations, and the terms of this Arrangement and irrelevant of the allocation of responsibilities agreed on in this Arrangement.

2.2 The Parties have determined the following processing activities as further described in their respective privacy notices:

Processing activity	Purpose of processing	Categories of processed data
Logging and storage of data	Logging technical data regarding the operation of the equipment along with the GPS position of the equipment and the identity of the operator for documentation and analysis purposes	• Identify of the operator • GPS position of the equipment during operations • Information on the settings of the equipment and data collected by the equipment about the process conditions.

2.3 The Parties shall store the personal data in a structured common and machine-readable format.

2.4 The Parties safeguard that only personal data is collected that is necessary for the legitimate handling of the respective processes for which data is collected.

3 Principles and legal basis

3.1 Data controller 2 is responsible for ensuring that all processing activities taking place under the joint controllership are in compliance with the fundamental principles as set out in article 5 of the General Data Protection Regulation, and that there is a valid legal basis for any and all processing activities.

3.2 Data controller 1 and Data controller 2 are both responsible for complying with the Principles for the Processing of Personal Data to the extent that the rules apply to the Data controller's responsibilities under this arrangement.

4 Rights of data subjects

4.1 Data controller 1 fulfils the information obligations towards the data subjects pursuant to Articles 13, 14 of the General Data Protection Regulation for the joint processing operations and takes the appropriate and necessary measures for this purpose. This includes reference to the applicable privacy notice of Data controller 2, containing information on Data controller 2's processing of personal data subject to this arrangement, including information on transfers to data processors and other third parties, and available at https://fremco.dk/privacy-policy/.

4.2 Data controller 1 fulfils the information and notification obligations under Articles 15 to 22 of the General Data Protection Regulation for the joint processing operations and takes the appropriate and necessary measures to ensure compliance with the following rules of the General Data Protection Regulation:

- the obligation to provide information when collecting personal data from the data subject,
- the obligation to provide further information if personal data have not been collected from the data subject,
- the data subject's right of access,
- the data subject's right of rectification,
- the right to erasure (right to be forgotten),
- the data subject's right to restriction of processing,
- the obligation to provide information in relation to the rectification or erasure of personal data or the restriction of processing,
- the data subject's right to data portability (except for public authorities);
- the data subject's right to object to processing; and
- the data subject's right to withdraw consent.

4.3 All practical handling of requests from data subjects shall be taken care of by Data controller 1.

4.4 If Data controller 2 receives a request or an enquiry from a data subject, it shall be transmitted to Data controller 1 as soon as possible in order for Data controller 1 to handle the further processing of the request.

4.5 Both Parties shall be responsible for mutually assisting each other to the extent appropriate and necessary for each of the Parties to comply with their obligations towards data subjects.

5 Security of processing and documentation of compliance with the General Data Protection Regulation

5.1 Data controller 2 will be responsible to implement appropriate technical and organisational measures to ensure and demonstrate that the processing is in compliance with the General Data Protection Regulation; taking into account the nature, scope, context and purposes of the processing involved, as well as the risks of varying degrees of likelihood and severity for the rights and freedoms of natural persons. The measures shall be documented, reviewed and updated as necessary (Article 24(1) sentence 2 of the General Data Protection Regulation).

5.2 The measures shall include, where proportionate to the processing activities, the implementation of appropriate data protection policies.

5.3 Data controller 2 shall be responsible for compliance with the data protection by design and data protection by default rule of Article 25 of the General Data Protection Regulation.

5.4 Data controller 2 is responsible for complying with the requirement of Article 32 of the General Data Protection Regulation on security of processing. This implies that Data controller 2, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing operation concerned, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure an appropriate level of security appropriate to those risks.

Data controller 2 shall carry out and document a risk assessment and then implement measures to mitigate the identified risks.

6 Use of data processors and sub-processors

6.1 Data controller 2 is entitled to use data processors and sub-processors in connection with the joint processing operation.

6.2 In the event of the use of processors and/or sub-processors, Data controller 2 shall be responsible for complying with the requirements of Article 28 of the General Data Protection Regulation. Accordingly, Data controller 2 shall, inter alia:

- use only processors that can provide the necessary guarantees that they implement appropriate technical and organizational measures in such a way as to ensure that processing complies with the requirements of this Regulation and safeguards the rights of the data subject,
- ensure that a valid data processing arrangement is in place between Data controller 2 and the processor; and
- ensure that there is a valid sub-processor arrangement between the processor and any sub-processor.

6.3 Data controller 1 shall be informed, upon request, whether the personal data is processed by processors and, where applicable, sub-processors of Data controller 2.

6.4 If personal data is processed by data processors and, where applicable, sub-processors, Data controller 1 shall be informed, upon request, of the content of the arrangements between Data controller 2 and the processor/sub-processor.

7 Records of processing activities

7.1 Data controller 2 shall be responsible for complying with the requirement of Article 30 of the General Data Protection Regulation on records of processing activities. This implies that Data controller 2 shall establish a record of the processing activities for which the Parties are joint controllers in respect of the associated processing of personal data.

7.2 Data controller 2 shall inform Data controller 1 of the content of the above record. The content of the above record as of the time of entering into this arrangement is included in Schedule 1.

7.3 Data controller 1 shall establish - based on the contents of the Data controller 2 record - its own record of the processing activities covered by the arrangement.

8 Notification of personal data breaches to the supervisory authority

8.1 Data controller 1 shall be responsible for compliance with Article 33 of the General Data Protection Regulation on the notification of personal data breaches to the supervisory authority for all data breaches related to the physical equipment for fiber blowing.

8.2 Data controller 2 shall be responsible for compliance with Article 33 of the General Data Protection Regulation on the notification of personal data breaches to the supervisory authority for all data breaches related to data stored in the Opticloud solution.

9 Communication of personal data breaches to the data subject

9.1 Data controller 1 shall be responsible for compliance with Article 34 of the General Data Protection Regulation regarding the communication of personal data breaches to the data subject, regardless of where the breaches occur. For breaches occurring in the Opticloud solution, Data controller 2 shall provide Data controller 1 with the information necessary to fulfil its obligations to inform the data subjects.

10 Data protection impact assessment and prior consultation

10.1 Data controller 2 shall be responsible for compliance with the requirement of Article 35 of the General Data Protection Regulation on data protection impact assessments. This implies that, where a type of processing, in particular using new technologies and by virtue of its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of natural persons, Data controller 2 shall, prior to the processing, carry out an analysis of the implications of the envisaged processing activities for the protection of personal data.

10.2 Data controller 2 shall also comply with the requirement of Article 36 of the General Data Protection Regulation to consult the supervisory authority in advance, where appropriate, including provision of the necessary information to the authority under Article 36(3) of the General Data Protection Regulation.

11 Transfer of personal data to third countries or international organizations

11.1 Data controller 2 may decide that personal data may be transferred to third countries or international organizations.

11.2 Data controller 2 shall be responsible for compliance with the requirements of Chapter V of the General Data Protection Regulation in the event of transfers of personal data to third countries or international organizations.

11.3 If Data controller 1 is located in a country outside the European Economic Area that is not recognized by the EU Commission as providing an adequate level of protection of personal data, the EU Standard Contractual Clauses in Schedule 2 shall apply for all transfers of data from Data controller 2 to Data controller 1 under this Joint Controllership Arrangement. For the sake of clarity, Schedule 2 shall not apply in situations, where Data controller 1 is located within the European Economic Area or in another country that is recognized by the EU Commission as providing an adequate level of protection of personal data.

12 Complaints

12.1 The Parties shall each be responsible for handling any complaints from data subjects, if the complaints relate to a breach of the provisions of the General Data Protection Regulation, for which the Party is responsible under this arrangement.

12.2 If one of the Parties receives a complaint, which should rightly be dealt with by the other Party, the complaint shall be forwarded to that controller as soon as possible.

12.3 If one of the Parties receives a complaint, part of which should rightly be dealt with by the other Party, that part shall be forwarded to the Party for reply as soon as possible.

12.4 The data subject shall be informed of the essential content of this arrangement when one Party forwards a complaint or part thereof to the other Party.

13 Informing the other Party

13.1 The Parties shall inform and liaise with each other of any material facts affecting the joint processing operation and this arrangement.

14 Regulation of other matters

14.1 Data controller 2 shall handle all practical matters in relation to processing of personal data subject to this Joint Data Controllership Arrangement, whether specifically described in the above clauses or not.

14.2 Data controller 2 shall be responsible for ensuring that all processing activities carried out under this Joint Data Controllership Arrangement are carried out in a manner that is compliant with the General Data Protection Regulation, including that documentation necessary to ensure compliance with the General Data Protection Regulation is produced.

15 Entry into force and termination

15.1 This Joint Data Controllership Arrangement shall enter into force upon being signed by both Parties.

15.2 The Joint Data Controllership Arrangement shall remain in force for as long as the personal data concerned are processed or until it is replaced by a new arrangement laying down the division of responsibilities in relation to the processing.

15.3 Signature

This arrangement is not signed separately, but considered entered into by both parties as an integral part of Data controller 1's creation of an Opticloud account.

Schedule 1

Information contained in the records of processing held by Data controller 2 in accordance with article 30 of the General Data Protection Regulation

Identity of the joint controllers	Data controller 1 and Data controller 2 as defined on the cover page of this agreement
Purpose of the processing	Collection and storage of log data from equipment manufactured by Data controller 2 and operated by Data controller 1 or persons assigned by Data controller 1 to operate the equipment
Categories of data subjects	Operators of the equipment
Categories of personal data	Identity of the operator GPS position of the equipment at the time of operation Settings of the equipment Technical data and measures recorded by the equipment during operations Comments entered in the log by the operator
Categories of recipients	Data processors: Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen Germany (Dedicated server) Sinch AB Lindhagensgatan 112 112 51 Stockholm Sweden (Sending of e-mails generated by the Opticloud system)
Transfers of personal data to third countries	N/A
Retention of personal data	Five years from the end of the calendar year in which the logging took place, unless otherwise specifically agreed.
Technical and organizational measures implemented pursuant to article 32 of the General Data Protection Regulation	Given the nature of the data processed, a security level that is **moderate** is determined to be sufficient. Data is stored in data centres in Germany providing (among other things): (a) Electronic physical entry control with logs (b) High security perimeter fencing (c) Video monitoring of entrances (d) Password protection (e) Formalized procedures for timely patching (f) Daily backup (g) Anti-virus and firewalls

Schedule 2

STANDARD CONTRACTUAL CLAUSES

Controller to Controller

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) N/A

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of

natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([4]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([5]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories

and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([6]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to

use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Denmark.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Fremco A/S
Company Registration Number 30 81 54 16
Ellehammervej 14
9900 Frederikshavn
Denmark
+45 72 30 12 13
support@fremco.dk

Activities relevant to the data transferred under these Clauses:

Logging of data as described in the joint controller agreement for which these Clauses form Schedule 2.

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

The company identified as Data controller 1 in the joint controller agreement for which these Clauses form Schedule 2.

Contact person's name, position and contact details: The OptiCloud Superuser – see contact information in OptiCloud account setup.

Activities relevant to the data transferred under these Clauses:

Logging of data as described in the joint controller agreement for which these Clauses form Schedule 2. Log data is intended to be used by the data importer for analysis and documentation purposes.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Operators of fiber blowing equipment manufactured by Fremco A/S and used by or on behalf of the data importer

Categories of personal data transferred

See Schedule 1 for the joint controller agreement for which these Clauses form Schedule 2.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Logging of settings and performance data of technical equipment.

Purpose(s) of the data transfer and further processing

Provision of log data to the data importer in order for the data importer to further use such data for analysis and documentation purposes.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Unless otherwise agreed, data will be retained for five years from the end of the year, the data was recorded.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data is transferred to the following sub-processor for storage

Hetzner Online GmbH
Industriestraβe 25
91710 Gunzenhausen
Germany

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Datatilsynet

Carl Jacobsens Vej 35
2500 Valby
Denmark
dt@datatilsynet.dk

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

All data is stored at a dedicated server at Hetzner Online GmbH, providing the following security measures:

- *Uniterruptable Power Supply (UPS) using redundant UPSs and emergency power supply system*
- *Redundant power supply from the substation*
- *Redundant and energy-efficient cooling using direct free cooling and climate controls*
- *Cold-aisle containment in above-average raised flooring*
- *Monitoring of process-relevant parameters via intelligent measurement, regulation, and monitoring system*
- *Sitewide early warning fire system; direct connection to the local fire and rescue coordination center*
- *Dynamic fire protection measures*
- *Regular training for emergencies and fire protection*
- *Redundant and highly available network infrastructure*
- *Continuous active DDoS recognition*
- *Individually configured firewall*
- *Data protection and information security management system (DMS, ISMS)*
- *Employment of a data protection and information security officer who is integrated into the operational processes*
- *Data-protection-friendly default settings (privacy by default and privacy by design)*
- *Incident response management*
- *Certifications according to ISO 27001, § 8a BSI-KritisV and BSI C5 Type 2 certification*
- *Annual review of TOMs by external service provider*
- *Annual review of the proper calculation and billing of connection charges by expert opinion in accordance with § 63 TKG*
- *EMAS certification (ISO 14001) of the environmental management system at German locations*

In addition, Fremco A/S is providing the following protectional measures:

- Automatic application of security-related software updates.
- Authentication of all user and administrative data accesses.
- Protective measures to mitigate denial of service attacks.
- Restrictive role-based internal access control.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation

(EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.