Data Controller You ("Data Controller"); and

Data Processor Leonh AB ("Data Processor")

Together referred to as the "Parties" and individually as a "Party".

BACKGROUND

The Agreement concerns the Personal Data processed in the context of the general terms and conditions of Leonh entered into by the Parties ("Terms"), under which the Data Processor processes personal data on behalf of the Data Controller.

In the event of any conflicts, this Agreement shall take precedence over the Terms.

DEFINITIONS

The terms used in the Agreement shall have the same meaning as set out in Article 4 of the General Data Protection Regulation.

"Processing" of personal data refers to any operation that can be performed on personal data, such as storage, alteration, reading, transfer, etc.

"Applicable Law" refers to the legislation applicable to the processing of personal data under the Agreement, including the General Data Protection Regulation, supplementary national legislation, as well as practices, guidelines, and recommendations issued by a Supervisory Authority.

"Personal Data" refers to any information that can be linked to an identifiable living person (in the Agreement, "Personal Data" is synonymous with "personal data for which the Data Controller is responsible and which the Data Processor processes on behalf of the Data Controller").

"Data Controller" refers to the company/organisation that determines the purposes and means of processing the personal data and thereby is responsible for ensuring that personal data is processed according to Applicable Law.

"Data Processor" refers to the company/organisation that processes personal data on behalf of the Data Controller and may therefore only process personal data according to the instructions of the Data Controller and Applicable Law.

"Data Subject" refers to the living person whose personal data is being processed.

"Supervisory Authority" means a Swedish or EU authority, such as the Swedish Data Protection Authority and, where applicable, another supervisory authority that by law oversees the Data Controller's activities.

Terms defined in the Terms shall have the same meaning in this Agreement.

INTRODUCTION

The Agreement governs the processing of personal data that the Data Processor carries out on behalf of the Data Controller. The Agreement has been drawn up to comply with the requirements set out in Article 28.3 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, and repealing Directive 95/46/EC ("General Data Protection Regulation"). According to this provision, a written agreement must be in place for the Data Processor's processing of personal data on behalf of the Data Controller.

DESCRIPTION OF THE PERSONAL DATA PROCESSING

Categories of Data Subjects

The Data Controller instructs the Data Processor to process data identifying the Data Controller's:

- Employees
- Customers
- Suppliers
- Consultants
- Business contacts
- Distributors
- Shareholders
- Board members

Categories of personal data

- Contact details
- Personal identity numbers
- Salaries

- Union membership
- Names

Source

The Data Processor processes the personal data that:

- Employees of the Data Controller enter into the Service
- The Data Controller collects from the Data Subjects

Purpose of the processing of personal data ("Purpose")

- To enable the Data Controller to manage legal matters and agreements through our digital platform

Processing of personal data

- Storage

DATA PROCESSOR'S SPECIAL COMMITMENTS

The Data Processor undertakes to, in connection with all processing, consider and observe the principles for the processing of personal data set out in Article 5 of the General Data Protection Regulation. Through the Agreement, the Data Processor guarantees that the Data Controller does not otherwise need to ensure that the Data Processor meets the requirements for expertise, reliability, and resources to implement the technical and organisational measures required under Applicable Law.

The Data Processor undertakes only to process personal data as provided by the Agreement, for the purposes set out in the Terms, according to the documented instructions of the Data Controller, and at all times under Applicable Law. The Data Processor shall, at the request of the Data Controller, assist the Data Controller through appropriate technical and organisational measures in their obligation to respond to requests to exercise the rights of Data Subjects and, considering the type of processing and the information available, carry out data protection impact assessments and prior consultations with the supervisory authority in accordance with Applicable Law. If the Data Processor violates Applicable Law by independently determining the purposes and means of the processing (e.g., processes the personal data for purposes other than the Purpose), the Data Processor shall be considered the data controller for the new processing without affecting the processing carried out in accordance with the Agreement otherwise. If the Data Processor considers the instructions provided

by the Data Controller to be incomplete, inadequate, or incorrect, the Data Processor shall immediately inform the Data Controller. The Data Processor also has the right to refrain from following the instructions of the Data Controller if they conflict with Applicable Law.

DATA CONTROLLER'S SPECIAL COMMITMENTS

The Data Controller determines the purposes and means of the processing of personal data. The Data Controller owns and has formal control over the personal data processed by the Data Processor. The Data Controller is responsible for the processing of personal data concerning the Data Subject. The Data Controller is responsible for ensuring that the personal data is accurate and up to date.

PERSONAL DATA BREACH

In the event of a situation leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data ("Personal Data Breach"), the Data Processor shall, without undue delay and no later than eight (8) hours after the Personal Data Breach has been discovered, inform the Data Controller in writing at the contact details provided. The information shall, to the extent available to the Data Processor, include at least the following:

- A description of the circumstances surrounding the Personal Data Breach
- A description of the nature of the Personal Data Breach, and, if possible, the categories and approximate number of Data Subjects affected, as well as the categories and approximate number of personal data records affected
- A description of the likely consequences of the Personal Data Breach
- A description of the measures taken or proposed to address the Personal Data Breach, and, where appropriate, measures to mitigate its potential adverse effects
- Contact details for the Data Protection Officer or other contact person who can provide more information to the Data Controller

If it is not possible for the Data Processor to provide the information at once, the information may be provided in stages without undue further delay.

AUDIT AND REVIEW

The Data Processor shall, at the request of the Data Controller, provide access to all information required to demonstrate that the Data Processor's obligations under Applicable Law and the Agreement have been fulfilled. If the information provided under the previous point cannot reasonably be considered sufficient to

demonstrate that the obligations set out under Applicable Law have been fulfilled, the Data Controller has the right to perform physical audits. The Data Processor shall enable and contribute to audits and inspections carried out by the Data Controller or an impartial third party appointed by the Data Controller. The Data Controller shall notify the Data Processor in writing of the planned audit at least ten (10) working days in advance.

The audit may only be carried out during normal business hours after the Data Controller has ensured that the person performing the audit is bound by a confidentiality agreement appropriate to the personal data and information being audited and in accordance with the Data Processor's internal policies and security procedures. Each Party shall bear its own costs incurred in connection with the audit. For any additional audits within one (1) year of the completed audit, the Data Controller shall bear all costs.

SUB-PROCESSOR

In cases where the Data Processor plans to engage a sub-processor or replace an existing sub-processor, the Data Processor shall inform the Data Controller at least five (5) working days in advance to give the Data Controller the opportunity to object to the change. If there are reasonable grounds for the Data Controller to object to a sub-processor, the Parties shall first cooperate to find an appropriate alternative, failing which the Data Controller has the right to terminate this Agreement and (if applicable) the Terms.

When engaging a sub-processor, the Data Processor shall ensure through a contract ("Sub-Processor Agreement") that the sub-processor has the same obligations as the Data Processor under the Agreement. This applies particularly concerning sufficient guarantees to implement the appropriate technical and organisational measures required to comply with Applicable Law. The Data Controller shall always have the right to access the Data Processor's sub-processor agreements (strictly commercial information may be redacted). The Data Processor shall maintain an up-to-date list of its sub-processors. The list shall be made available to the Data Controller upon request.

If the sub-processor fails to fulfil its obligations under the Sub-Processor Agreement, the Data Processor shall be fully responsible to the Data Controller for the sub-processor's actions or failure to act.

REGISTER AND DATA PROTECTION OFFICER

The Data Processor undertakes to maintain a written record of the processing of personal data containing the information set out in Article 30.2 of the General Data Protection Regulation. The record shall be made available to the Data Controller upon request. If the processing or nature of the business requires the Data Processor to appoint a Data Protection Officer in accordance with Article 37 of the General Data Protection Regulation.

CONTACT WITH THE SUPERVISORY AUTHORITY AND THE DATA SUBJECT

The Data Processor shall promptly inform the Data Controller of any contact with the Data Subject, supervisory authority, or any other third party regarding the Data Processor's processing of the personal data. If the Data Subject makes a request to the Data Processor concerning their rights related to the processing, the Data Processor shall refer the Data Subject to the Data Controller. The Data Processor shall allow inspections required by the supervisory authority in accordance with Applicable Law. The Data Processor does not have the right to represent the Data Controller or otherwise act on behalf of the Data Controller in relation to the Data Subject, supervisory authority, or any other third party.

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

The Data Processor shall take appropriate organizational and technical security measures to protect the personal data covered by the Agreement from unauthorized or unlawful access. This includes ensuring sufficient capacity, technical solutions, competence, financial and personnel resources, procedures, and methods. The adequacy of the technical and organizational security measures shall be assessed considering the latest developments, implementation costs, and the nature, scope, context, and purpose of the processing, as well as the risk posed to fundamental rights and freedoms by the processing. If the Data Controller assesses the risk level of the processing as high and thereby conducts a data protection impact assessment, the Data Controller shall share the result of the assessment with the Data Processor so that it can be taken into account when determining what constitutes appropriate security measures. The Data Processor shall comply with any decisions and consultations issued by the supervisory

authority regarding measures to meet the security requirements under Applicable Law and all other requirements applicable to the Data Processor under Applicable Law. The Data Processor shall ensure that employees (of the Data Processor or its subcontractors) only have access to personal data to the extent necessary and that those who have access to personal data have committed to maintaining the confidentiality of such information (e.g., by signing an individual confidentiality agreement). Only persons employed/engaged as consultants by the Data Processor who are deemed to have the necessary level of knowledge in relation to the nature and scope of the personal data processing may process the personal data. Computer equipment, storage media, and other equipment used in the processing of personal data carried out by the Data Processor shall be stored in such a way that unauthorized persons cannot access them. The security of the Data Processor's premises where personal data is processed shall be appropriate and secure with regard to locking equipment, functioning alarm equipment, protection against fire, water, and burglary, and protection against power failures and disturbances. The equipment used for processing personal data shall be well protected against theft and events that may destroy the equipment and/or personal data.

CONTROL OVER PERSONAL DATA

The Data Processor shall ensure that the Personal Data is not accidentally or unlawfully destroyed, altered, or falsified. The data shall be protected against unauthorized access during storage, transfer, and other processing. Personal data may only be provided to the Data Controller after secure identification of the recipient.

TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA

The Data Processor primarily processes the Personal Data within the EU/EEA. In cases where the personal data is not processed within the EU/EEA, the Data Processor shall ensure that the processing is lawful under Applicable Law by fulfilling one of the following requirements:

- There is a decision from the EU Commission that the country ensures an adequate level of protection.
- The Data Processor applies the EU Commission's standard contractual clauses for the transfer of data to third countries.
- The Data Processor has taken other appropriate safeguards that comply with Applicable Law.

LIABILITY AND COMPENSATION

A Party is exempt from liability for obligations under the Agreement in cases where fulfillment is hindered by circumstances of an extraordinary nature beyond the Party's control, which the Party could not reasonably have been expected to foresee and the consequences of which the Party could not reasonably have avoided or overcome. The Data Processor is liable for direct damages resulting from the Data Processor processing personal data in violation of the Data Controller’s instructions according to the Agreement and Applicable Law. The Data Processor shall compensate the Data Controller for direct damage, up to a maximum of 50,000 SEK. Compensation shall not be paid if the claim is related to processing that has been approved or carried out according to the Data Controller’s instructions. The Data Processor is not liable for the Data Controller’s legal costs. The Data Processor’s liability shall not cover indirect damages or consequential damages such as lost income or profits, contracts, customers, or business opportunities, loss of goodwill, or expected savings.

CONFIDENTIAL INFORMATION

The Data Processor may not use information or other material to which it has access within the framework of the Agreement or the Terms for any other purpose than to fulfill obligations under this Agreement or the Terms. The Data Processor may not disclose or reveal to third parties or any unauthorized persons information about the processing of personal data or the content of personal data covered by this Agreement, or any other information to which the Data Processor has access as a result of this Agreement. This does not apply to information that the Data Processor is obliged to disclose by law. The confidentiality obligation is valid from the day both Parties sign the Agreement and indefinitely thereafter. The Data Processor shall ensure that the confidentiality obligation applies to all employees and other persons working for or on behalf of the Data Processor who are authorized to process personal data.

TERM AND TERMINATION

The Agreement is valid as long as the Data Processor processes personal data on behalf of the Data Controller or until the Agreement is replaced by another data processing agreement. The Data Processor’s obligations under the Agreement shall continue to apply, regardless of whether the Agreement has been terminated or otherwise ceased to be valid, as long as the Data Processor processes personal data on behalf of the Data Controller.

DELETION AND RETURN OF PERSONAL DATA

Upon termination of the Agreement, the Data Processor and any sub-processors shall either delete or return the personal data covered by the Agreement.

APPLICABLE LAW AND DISPUTE RESOLUTION

Swedish law shall apply to this Agreement. The dispute resolution mechanism set out in the Terms shall also apply to this Agreement.

APPLICABLE LAW AND DISPUTE RESOLUTION

Swedish law shall apply to this Agreement. The dispute resolution mechanism outlined in the Terms shall also apply to this Agreement.

LEONH'S PROCESSING OF PERSONAL DATA

Legal Grounds
Legitimate Interest - Leonh may process personal data if we have assessed that there is a legitimate interest that outweighs the Data Subject's right to privacy and if the Processing is necessary for the relevant purpose.

How Long Do We Retain Your Personal Data?
We retain your Personal Data for as long as necessary considering the purpose for which it was collected. Depending on the legal ground we rely on for the processing, this may a) arise from a contract, b) depend on valid consent, c) be required by legislation, or d) follow from an internal assessment based on a legitimate interest. Below, we specify (where possible) the period for which Personal Data will be stored or the criteria used to determine the period.

Processing Activities

1. **Processing and Purpose:** Register user account to allow the customer's employees to log in and access the Service.
    - **Personal Data:** Name, email address, company.
    - **Source:** Directly from the Data Subject.
    - **Legal Ground:** Legitimate interest in providing the Service according to the agreement with the customer.

    - **Retention Period:** As long as the Data Subject has access to a user account linked to a customer.
2. **Processing and Purpose:** Register user account linked to a trial account to allow the customer's employees to log in and test the Service.
    - **Personal Data:** Name, email address, company.
    - **Source:** Directly from the Data Subject.
    - **Legal Ground:** Legitimate interest in presenting the Service to convert the customer into a paying customer.
    - **Retention Period:** One year from the creation of the user linked to the trial account.
3. **Processing and Purpose:** Verify the user's login credentials to increase security and prevent abuse.
    - **Personal Data:** Name, email address.
    - **Source:** Directly from the Data Subject.
    - **Legal Ground:** Legitimate interest in verifying the user's identity to enhance security and prevent misuse of the Service.
    - **Retention Period:** As long as the Data Subject has access to a user account linked to a customer.
4. **Processing and Purpose:** Communicate to effectively assist customers with any issues (customer support) and provide relevant information about the Service.
    - **Personal Data:** Name, email address, phone number, company.
    - **Source:** Directly from the Data Subject.
    - **Legal Ground:** Legitimate interest in providing the Service according to the agreement with the customer and increasing and maintaining customer satisfaction.
    - **Retention Period:** As long as the Data Subject has access to a user account linked to a customer.
5. **Processing and Purpose:** Marketing and information efforts to attract and retain potential customers for the Service.
    - **Personal Data:** Name, email address, phone number, company.
    - **Source:** Directly from the Data Subject and sourcing from publicly available sources (LinkedIn, potential customer websites, etc.) and third parties.
    - **Legal Ground:** Legitimate interest in increasing sales and conducting our business.
    - **Retention Period:** Two years or until the Data Subject unsubscribes from email communications.
6. **Processing and Purpose:** Marketing and information efforts to retain and upgrade existing customers.
    - **Personal Data:** Name, email address, phone number, company.
    - **Source:** Directly from the Data Subject.

    - **Legal Ground:** Legitimate interest in creating a long-term customer relationship where we provide value to the customer over time.
    - **Retention Period:** As long as the Data Subject has access to a user account linked to a customer or until the Data Subject unsubscribes from email communications.
7. **Processing and Purpose:** Collecting (sourcing) contact details of potential customers.
    - **Personal Data:** Name, email address, phone number, company.
    - **Source:** Sourcing from publicly available sources (LinkedIn, potential customer websites, etc.) and third parties.
    - **Legal Ground:** Legitimate interest in increasing sales and conducting our business.
    - **Retention Period:** Three months.
8. **Processing and Purpose:** Retain information about Data Subjects who have unsubscribed from information communications to avoid sending similar unwanted emails in the future.
    - **Personal Data:** Email address.
    - **Source:** Directly from the Data Subject.
    - **Legal Ground:** Legitimate interest in complying with applicable law and meeting the Data Subject's request.
    - **Retention Period:** Two years.
9. **Processing and Purpose:** Compile statistics and analyses to improve the Service and user experience as well as for business purposes.
    - **Personal Data:** Email address, IP address, browser.
    - **Source:** Generated internally.
    - **Legal Ground:** Legitimate interest in improving and developing the Service.
    - **Retention Period:** 7 days.

Your Rights

You control your Personal Data. We always strive to ensure that you can exercise your rights as effectively and smoothly as possible.

- **Access:** You have the right to obtain information about the Personal Data we process about you. We will only provide information if we can verify that it is indeed you requesting the data.
- **Rectification:** If you discover that the Personal Data we process about you is incorrect, contact us and we will correct it!
- **Erasure:** You have the right to request the deletion of your Personal Data when it is no longer necessary for the purposes for which it was collected. If we are required to retain your data according to law or an agreement with

you, we will ensure that it is only processed for the specific purpose outlined by law or contract, and then delete it as soon as possible.

- **Objection:** If you disagree with our assessment that our interest in processing your Personal Data outweighs your interest in privacy protection, we will review our interest assessment and check if it still holds. We will of course take your objection into account when making a new assessment to determine if we can still justify our processing of your Personal Data. If you object to direct marketing, we will immediately remove your Personal Data without reviewing our assessment.
- **Restriction:** You may also ask us to restrict our processing of your data:
  - While we handle a request from you regarding any of your other rights.
  - If you, instead of requesting deletion, want us to mark the data so it is not processed for a specific purpose. For example, if you do not want us to send you advertising in the future, we still need to retain your name to know not to contact you.
  - In cases where we no longer need the data for the purpose it was collected for; provided that you do not have an interest in us retaining the data to assert a legal claim.
- **Data Portability:** We can provide you with the data you have provided to us or which we have received from you in connection with an agreement with you. You will receive your data in a commonly used and machine-readable format that you can then take to another Data Controller.
- **Withdraw Consent:** If you have consented to one or more specific processing activities of your Personal Data, you have the right to withdraw your consent at any time and request that we cease the processing immediately. Please note that you can only withdraw your consent for future processing of Personal Data and not for any processing that has already occurred.

Transfer of Personal Data

To conduct our business, we may need to enlist others to process Personal Data on our behalf, so-called Data Processors.

In cases where our Data Processors transfer Personal Data to a country outside the EU/EEA, we ensure that the processing is legal according to applicable law by meeting one of the following requirements:

- There is a decision by the EU Commission that the country ensures an adequate level of protection;

- Application of EU Commission's Standard Contractual Clauses for third-country transfers; or
- Other appropriate safeguards that meet applicable law.

We have entered into Data Processing Agreements (DPAs) with all our Data Processors. The DPA regulates how the Data Processor may process Personal Data and the security measures required for the data processing.

We may also need to disclose your Personal Data to certain designated authorities to fulfill obligations under law or governmental decisions.

Transfer of Personal Data to Another Data Controller

When our customers request "Legal Support," they are referred to one of our partners. To streamline the process regarding Know Your Customer (KYC) and conflict of interest, we collect personal data on behalf of our partner.

For more information on what this entails, see the current partner’s privacy policy.

Security

Leonh has implemented technical and organizational measures to ensure that your personal data is processed securely and protected from loss, misuse, and unauthorized or unlawful access.

Our Security Measures

Organizational security measures are actions implemented in organizational procedures and practices. Our organizational security measures include:

- Internal documents (policies/instructions)
- Information Security Policy
- Physical security (premises, etc.)

Technical security measures are actions implemented through technical solutions. Our technical security measures include:

- Encryption
- Access lists
- Access logs
- Secure networks
- Regular security level checks

- Two-factor authentication
- Password management program for all passwords

Cookies

Leonh uses cookies and similar tracking technologies to, among other things, analyze how Features are used to provide you with the best possible user experience. For more information about how we use cookies, please see our Cookie Policy.

Changes to This Policy

We reserve the right to make changes to this Policy. If the change affects our obligations or your rights, we will inform you of the changes in advance