Data Processing Agreement

This data processing agreement, (the "Agreement"), forms an integral part of Expandra ABs, (the "Processor") Terms of Service related to the Proposal Service Expandra, (the "Terms"). Any term not otherwise defined herein shall have the meaning ascribed to it in the Terms.

1. Background

1.1 The Processor will process personal data within the scope of the Service on behalf of the legal entity, represented by you, that has accepted and executed the Terms. The legal entity is, therefore, the "Controller" with respect to this Agreement.

1.2 The Controller and the Processor are each a "Party" and collectively the "Parties".

1.3 In light of the above, the Parties have reached the following Agreement.

2. Relationship Between the Agreement and other Agreements Between the Parties

In the event that the provisions of this Agreement contradict the provisions of any other agreement between the Parties, the provisions of this Agreement shall prevail. However, the foregoing does not apply to provisions of a subsequent agreement that expressly supersede the provisions of this Agreement.

3. Processing of Personal Data

3.1 In the context of performing the Service, the Processor may receive personal data, as defined in article 4.1 of the General Data Protection Regulation (EU 2016/679) (the "GDPR"), processed for purposes determined by the Controller (the "Personal Data"). The Controller is the data controller of the Personal Data by the personal data protection laws applicable from time to time, as well as any other applicable law, regulation, or equivalent ordinance.

3.2 The Processor undertakes to only process the Personal Data by the terms of the Agreement or other written Agreement between the Parties, and only by the Controller's instructions, Appendix 1, as well as with the from time to time applicable data protection legislation and any other applicable law, regulation or equivalent ordinance. The Controller is responsible for ensuring that the Processor does not process any other categories of Personal Data than those listed in Appendix 1 and by the scope stated therein. In case of changes in the documented instructions by the Controller, the Processor is entitled to reasonable compensation.

3.3 In case the Processor lacks the instructions that the Processor considers necessary to perform the tasks that the Processor has acquired from the Controller within the scope of the Service, the Processor shall, without delay, notify the Controller of its position and await such instructions that the Controller deems necessary.

3.4 Access to the Personal Data shall, within the Processor's organization, be limited to those who require it for the performance of the Service and who are obligated to observe secrecy by Agreement or by law. The Processor shall take appropriate technical and organizational measures to protect the Personal Data. Such measures shall provide a level of security appropriate with regard to the available technology and the cost of the measures, taking into account whether there are any specific risks involved with the processing and the level of sensitivity of the Personal Data. Such measures include:

– the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

– the ability to restore the availability of and access to the Personal Data in a timely manner in the event of a physical or technical incident;

– the pseudonymization and encryption of the Personal Data when the processing so requires under the applicable law;

– a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing, when required under the applicable law;

– keeping and updating logs of Personal Data; maintaining a secure IT environment, and establishing and maintaining physical security measures and procedures; and

– ensuring procedures to immediately notify the Controller at every attempt at or complete unauthorized access to the data provided by the Controller (including destruction or alteration of the Personal Data).

3.5 The Processor undertakes to ensure that relevant personnel comply with this Agreement and the

Controller's instructions at all times and that they are kept informed regarding the applicable data protection legislation from time to time.

3.6 The Processor shall, through suitable technical and organizational measures and to the degree it is possible about the nature of the processing, assist the Controller for the Controller to be able to fulfill its obligation to respond to requests from the individual data subjects by the applicable law or regulation. The Processor shall also, in all other aspects, assist the Controller in fulfilling its obligations, taking into account the type of processing and the information available to the Processor regarding

– security in connection to the processing;
– notification of any personal data breach to the supervisory authority;
– communication to the data subject of a personal data breach, and
– data protection impact assessment and prior consultation;

to the extent that the obligations in (a)-(d) above are required according to the applicable law or regulation. The Processor shall be entitled to reasonable compensation for its assistance in accordance with this Section 3.6.

3.7 The Processor undertakes to maintain a written record of the processing of Personal Data, including the content stated in Article 30.2 of the GDPR. Upon request, the records shall be provided to the Controller.

3.8 If contrary to the GDPR, the Controller does not inform the individual data subject of a personal data breach and the supervisory authority orders the Processor to rectify the deficiency, the Controller

shall compensate the Processor's costs to adhere to the order of a supervisory authority.

3.9 The Processor can appoint another processor (a so-called sub-processor) to process Personal Data. The Processor shall inform the Controller that the Processor intends to appoint another or replace a sub-processor at least ten (10) working days before such an appointment or replacement occurs. If the Controller objects to the appointment of such sub-processor that the Controller has been informed of according to this Section 3.9 before the appointment, the Processor cannot appoint the sub-processor for the processing of the Personal Data, provided that the Controller had a justifiable reason for its objection. The term "justifiable reason," as referred to in this Section, refers to circumstances on behalf of the sub-processor that, to a considerable degree, affects, or likely will affect, the protection of the personal integrity of the individual data subject for example, if the new sub-processor does not fulfill the requirements on personal data processors in the GDPR or any other relevant privacy legislation. If the Processor engages such sub-processor, the Processor shall ensure that the data processor by Agreement undertakes the same data privacy obligations arising from this Agreement. The Processor is fully responsible to the Controller for such undertakings of the sub-processor.

3.10 Unless otherwise agreed upon in writing between the Parties, the Processor has the right to transfer personal data outside the EU/EEA. The Processor undertakes to only transfer or process personal data outside the EU/EEA when such transfer or processing is lawful under article 45-47 of the GDPR.

3.11 The Controller has the right to

information and audit the performance of the Processor's obligations under the Agreement. The Processor shall allow and contribute to such audits, including inspections, carried out by the Controller or an auditor engaged by the Controller. Suppose the Controller wishes to carry out an inspection. In that case, the Controller shall inform the Processor of such inspection within reasonable time before the inspection and, at the same time, specify the content and scope of the inspection. The Processor has the right to compensation for its reasonable costs in relation to such an inspection or other audit. Unless otherwise agreed upon in writing, the inspection can only be performed if an audit according to the GDPR cannot be fulfilled through the provision of information by the Processor.

3.12 According to Section 3.11, an inspection requires that the Controller, or an auditor appointed by the Controller, has agreed upon necessary confidentiality obligations and adheres to the safety regulations at the inspection place. It also requires that the inspection is performed without the risk of disrupting the Processor's business operations or the protection of the information of other controllers and personal data. Information gathered as part of an audit, including inspections, shall be deleted after the audit is completed or when it is not necessary for the purpose of the audit.

3.13 The Processor shall immediately inform the Controller if it believes that an instruction is contrary to applicable law, regulation, or equivalent ordinance. The Processor shall be prepared to comply with decisions made by the Swedish Data Protection Authority on measures to comply with the safety requirements

of applicable law.

3.14 The Processor shall, without delay, notify the Controller regarding any contact with a competent supervisory authority that concerns or could be of importance for the Processor's processing of Personal Data. The Processor does not have the right to represent the Controller or act on its behalf in relation to the supervisory authority.

3.15 Upon discontinuation of the Processor's processing of the Personal Data (e.g., due to the Controller giving instructions that the processing should be discontinued or that the Agreement is terminated in accordance with Section 4.1 below), the Processor shall return all data containing personal data covered by this Agreement and all media on which such data is stored. The Processor shall also delete existing copies of all such data, e.g., from backup systems unless the Processor has a legal obligation to retain the Personal Data under union or member state law.

4. Miscellaneous

4.1 This Agreement shall enter into force upon signing by authorized representatives of both Parties. The Agreement shall terminate simultaneously with the Agreement between the Parties governing the Service; however, it shall be at the earliest when the Processor has ceased all processing of the Personal Data.

4.2 The Processor has no right to transfer its rights or obligations under this Agreement, in whole or in part, without the Controller's prior written consent.

4.3 If applicable data protection legislation changes during the period of this Agreement, or if a competent supervisory authority issues guidelines, decisions, or rules regarding the application of the applicable data protection legislation, that results in this Agreement no longer meet the requirements provided for data processing agreements, or if the Agreement or agreements that regulate the Service change, this Agreement shall change to accommodate such new or additional requirements and changes. Any such change shall enter into force on the day that the Controller states, but not before five days after notice of such change was sent to the Processor. The Processor has the right to compensation for the reasonable costs incurred by such a change of this Agreement.

4.4 In addition to what is applicable under the Agreement or agreements that regulate the Service, for the period of this Agreement and thereafter, the Processor undertakes not to disclose the Personal Data to any third party. The Personal Data may only be disclosed to such employees of the Processor for which the Personal Data is necessary to perform their tasks, to a competent supervisory authority, or otherwise when disclosure of the Personal Data is required by law. It is the Processor's responsibility to ensure that employees likely to come in contact with the Personal Data have undertaken to keep the Personal Data confidential to the same extent as the Processor is required under this Agreement.

4.5 This Agreement shall be governed by and construed by Swedish law. Disputes concerning the interpretation or application of this Agreement shall be settled in accordance with the Agreement or agreements between the Parties governing the Service.

Appendix 1: Controller's instructions

Below are the Controller's instructions, as stated in Section 3.2 of the Agreement. Instructions given at a later date that make reference to the Agreement replace the ones provided below.

Categories of Data Subjects

Potential customers and receivers of the Controller's proposal.

Types of Personal Data

Name, email address, company name, address for invoicing, phone number, data on the use of the Service, time of acceptance or rejection of a proposal, and other potential data contained in the proposal or related to the proposal.

Processing Purposes

The Personal Data may only be processed for the following purposes and only on behalf of the Controller: Providing the Service, including sending, following up, and registering the acceptance or rejection of a proposal.

Nature of the Processing

Storage, viewing, transferring, registering, amending, deleting.

Retention Period

As long as necessary for the provision of the Service, always at most until the Controller instructs the Processor to delete the Personal Data (some or all).

Sub-Processors

The Processor may, provided the conditions in Section 3.9 are met, transfer the Personal Data to any sub-processor. Approved sub-processors at the date of this Agreement are:
1. Itrera AB
2. Akamai Technologies
3. Amazon AWS
4. Helpscout
5. 37 Signals

Third Country Transfers

The Processor may, provided that the conditions in Section 3.10 are met, transfer the Personal Data to countries outside the EU/EEA.