DATA PROCESSING AGREEMENT

Effective August, 2021

PARTIES

(1) The customer entity that is a party to the Master Agreement **(**further **"Controller")** and

(2) **ProfitSoft B.V.**, a Dutch company with limited liability **(**further **"Processor")**.

BACKGROUND

(A) Controller and Processor entered into Expandi's Terms & conditions (**Master Agreement**), which govern Controller's use of Expandi platform provided by Processor;

(B) Due to the scope and subject matter of the Master Agreement, it is necessary for the Processor to process Personal Data on behalf of Controller.

(C) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which Processor will process Personal Data under the Master Agreement. This Agreement is an integral part of the Master Agreement and contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between data controllers and data processors.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that Controller authorises to give Processor personal data processing instructions.

Data Subject: an individual who is the subject of Personal Data.

Personal Data: means any information relating to an identified or identifiable natural person that is processed by Processor as specified in ANNEX A; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing, processes and process: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.

Data Protection Legislation: all applicable privacy and data protection laws including the General Data Protection Regulation ((EU) 2016/679) and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

SCC: the European Commission's Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU).

1.2 Any reference to 'writing' or 'written' includes faxes, email and electronic messaging service.

1.3 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in Annex A, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in Annex A, the provision contained in Annex A will prevail.

2. Personal data types and processing purposes

2.1 Controller and Processor acknowledge that as per definitions in the Data Protection Legislation, Controller is the Controller and Processor is the Processor.

2.2 Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Processor.

2.3 ANNEX A describes the subject matter, duration, nature and purpose of processing, Personal Data categories, Data Subject categories in respect of which Processor may process Personal Data, as well as the relevant security measures to be taken by Processor.

2.4 ANNEX B provides the list of subprocessors involved by Processor.

3. Processor's obligations

3.1 Processor will only process the Personal Data in accordance with Controller's written instructions specified in Annex A. Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or Data Protection Legislation. Processor must promptly notify Controller if, in its opinion, Controller's instruction would not comply with Data Protection Legislation.

3.2 Processor must promptly comply with any of Controller's requests or instruction from Authorised Persons requiring Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless Controller or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires Processor to process or disclose Personal Data, Processor must first inform Controller of the legal or regulatory requirement and give Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 Processor will reasonably assist Controller with meeting Controller's compliance obligations under Data Protection Legislation, taking into account the nature of Processor's processing and the information available to Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.5 Processor must promptly notify Controller of any changes to Data Protection Legislation that may adversely affect Processor's performance of the Master Agreement.

3.6 **Processor's employees**

3.7 Processor will ensure that all employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

3.8 Processor will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable law on all of Processor's employees with access to the Personal Data.

4. Security

4.1 Processor must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data.

4.2 Processor must implement such measures in accordance with Art. 32 of the General Data Protection Regulation (*(EU) 2016/679*), to ensure a level of security appropriate to the risk involved.

4.3 Controller hereby confirms that organisational and technical measures specified in Annex A are sufficient and appropriate under the Data Protection Legislation and this Agreement.

5. Personal Data Breach

5.1 Processor will promptly and without undue delay notify Controller if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. Processor will restore such Personal Data at its own expense.

5.2 Processor will immediately and without undue delay notify Controller if it becomes aware of:

(a) any accidental, unauthorised or unlawful processing of the Personal Data; or

(b) any Personal Data Breach.

5.3 Where Processor becomes aware of (a) and/or (b) of clause 5.2, it shall, without undue delay, also provide Controller with the following information:

(a) description of the causes and nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

5.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will coordinate with each other to investigate the matter. Processor will reasonably cooperate with Controller in Controller's handling of the matter, including:

(a) assisting with any investigation;

(b) providing Controller with physical access to any facilities and operations affected;

(c) facilitating interviews with Processor's employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by Controller; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

5.5 Processor will not inform any third party of any Personal Data Breach without first obtaining Controller's prior written consent, except when required to do so by law.

5.6 Processor agrees that Controller has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in Controller's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

5.7 Processor will cover all reasonable expenses associated with the performance of the obligations under clause 5.2 and clause 5.4 unless the matter arose from Controller's specific instructions, negligence, wilful default or breach of this Agreement, in which case Controller will cover all reasonable expenses.

6. Cross-border transfers of personal data

6.1 Controller hereby authorises Processor to transfer or otherwise process Personal Data outside the European Economic Area (**EEA**) subject to conditions laid down in this Agreement.

6.2 Processor may only process, or permit the processing, of Personal Data outside the EEA under one of the following conditions:

(a) Processor is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. Processor must identify in an additional annex hereto the territory that is subject to such an adequacy finding;

(b) Processor takes, where appropriate, one of the safeguards specified by Data Protection Legislation, notably by Article 46 of the General Data Protection Regulation *(EU) 2016/679*).

6.3 If any Personal Data transfer between Controller and Processor requires execution of SCC in order to comply with the Data Protection Legislation (where Controller is the entity exporting Personal Data

to Processor outside the EEA), the parties will complete all relevant details and take all other actions required to legitimise the transfer.

7. Subprocessors

7.1 Processor may not authorise a third party (subprocessor) to process the Personal Data unless all of the following conditions are met:

(a) Controller has given a specific or general authorisation to the engagement of the subprocessor(-s);

(b) Processor enters into a written contract with each of the authorised subprocessors that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures;

(c) Processor maintains control over all Personal Data it entrusts to the subprocessor(-s).

7.2 Controller hereby gives a general authorisation to involve subprocessors to process personal data under this Agreement. In the case Processor intends to update the list of subprocessors engaged, he must inform Controller and provide Controller with the opportunity to object against the intended changes.

7.3 Where the subprocessor fails to fulfil its obligations under such written agreement, Processor remains fully liable to Controller for the subprocessor's performance of its agreement obligations.

7.4 Where Processor fails to fulfil its guarantees under clause 7.1, it shall indemnify all of the Controller’s arising direct and indirect damages.

8. Complaints, data subject requests and third-party rights

8.1 Processor must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to Controller as Controller may reasonably require, to enable Controller to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

(b) information or assessment notices served on Controller by any supervisory authority under the Data Protection Legislation.

8.2 Processor must notify Controller immediately and without undue delay if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

8.3 Processor must notify Controller immediately and without undue delay when it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

8.4 Processor will give Controller its full cooperation and assistance in responding to any complaint, notice, communication or Data Subject request in connection with Personal Data processed.

8.5 Processor must not disclose the Personal Data to any Data Subject or to a third party other than at Controller's request or instruction, as provided for in this Agreement or as required by law.

9. Term and termination

9.1 This Agreement will remain in full force and effect so long as:

(a) the Master Agreement remains in effect, or

(b) Processor retains any Personal Data related to the Master Agreement in its possession or control (**Term**).

9.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Data will remain in full force and effect.

9.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 2 (two) months, they may terminate the Master Agreement on written notice to the other party.

10. Data return and destruction

10.1 At Controller's request, Processor will give Controller a copy of or access to all or part of Controller's Personal Data in its possession or control in the format and on the media reasonably specified by Controller.

10.2 On termination of the Master Agreement for any reason or expiry of its term, Processor will securely delete or destroy or, if directed in writing by Controller, return and not retain, all or any Personal Data related to this Agreement in its possession or control.

10.3 If any law, regulation, or government or regulatory body requires Processor to retain any documents or materials that Processor would otherwise be required to return or destroy, it will notify Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

10.4 Processor will certify in writing that it has destroyed the Personal Data within 30 days after it completes the destruction.

11. Audit

11.1 If Controller is required to show its compliance with Data Protection Legislation, reasonably believes that a Personal Data Breach occurred or is occurring, or Processor is in breach of any of its obligations under this Agreement or any Data Protection Legislation, Processor will permit an assigned and eligible third-party representative of the Controller to audit Processor's compliance with this Agreement obligations, on at least 30 (thirty) days' notice, during the Term. Processor will give the third-party representative of the Controller all necessary assistance reasonably required to conduct such audits, provided that the audit concerns only the activities described in Annex A, and Controller and its third-party representatives keep confidentiality over the information obtained throughout the audit. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to any information held at Processor's premises or on systems storing Personal Data;

(b) access to and meetings with any of Processor's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) necessary inspection of all infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

11.2 If a Personal Data Breach occurs or is occurring, or Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, Processor will:

(a) promptly conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide Controller with a copy of the written audit report; and

(d) promptly remedy any deficiencies identified by the audit.

11.3 Processor will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by Processor's management.

11.4 Controller will cover all reasonable expenses incurred by Processor in connection with performing its obligations under clause 11.1.

ANNEX A Personal Data Processing Purposes and Details

Subject-matter and nature of processing: the provision of automation services for marketing on LinkedIn social network (https://linkedin.com, further referred to as "**LinkedIn**"), which requires the processing of personal data of LinkedIn registered users by Processor on behalf of Controller.

The nature of the processing activities implies the search, collection, and structuring of information from the profiles of LinkedIn users, as well as the creation and automated sending of messages to LinkedIn users on behalf of Controller and/or Controller representatives.

Duration of Processing: duration of the Master Agreement.

Categories of data subjects: registered users of LinkedIn.

Purposes	**Personal data categories**
To allow Controller to prepare and conduct LinkedIn marketing activities	Profile photo, name, occupation, company, url, inbox messages, date and time of the message
To allow Controller to find people from its LinkedIn connections	Profile link, profile picture, full name, status (contact / new contact / ex-contact / connection sent) type of connection (1st / 2nd / 3rd), occupation, tags, connected since, campaign assigned, filter words from profile
To allow Controller to automate interactions with LinkedIn contacts	Inbox messages, connection status (contact / new contact / connect requested), message status (email required / no interaction / awaiting reply / replied) name of message recipient, date and time when the message was sent
To allow Controller to find people on LinkedIn	Profile picture, name, occupation, company, url, post engagement, post author
To allow Controller to track the status of its connection requests on LinkedIn	Profile picture, name, occupation, tags, actions
To allow Controller to sort its LinkedIn connections	Name, marketing campaign affiliation, tags, actions to be done
To allow Controller to integrate third-party tools	LinkedIn Controller data from Expandi and a third-party tool: name, event, campaign, tags, target url, history, time delta, test
To allow Controller to import its LinkedIn contacts and blacklists to Processor's platform	Contact id, first name, last name, profile link, job title, company name, email, phone, address, image link, tags, contact status, conversation status, object urn, public identifier, profile link public identifier, message thread link, invited at, connected at
To allow Controller to analyse whether a LinkedIn contact responded to its message positively	Conversation status (success / failure)
To allow Controller to export LinkedIn contacts found via Processor's platform	Contact id, first name, last name, profile link, job title, company name, email, phone, address, image link, tags, contact status, conversation status, object urn, public identifier, profile link public identifier, message thread link, invited at, connected at
To allow Controller to analyse the efficiency of its social/marketing activities on LinkedIn	Day-by-day (periodical) statistics, total statistics, communication statistics, campaign statistics, task statistics based on personal data listed above

Security measures:

- Monitoring of API endpoints;
- Limitation and management of access rights to personal data;
- SSH protocol for accessing LinkedIn login data;
- 2FA to employee accounts;
- 2FA feature for user accounts;

- Database encryption at-rest;
- VPN for accessing servers;
- Secure (https://) connection;
- Compliance with password protection and management, access control policies;
- Usage of antivirus software and firewalls;
- Employees are aware of and trained on their respective data protection responsibilities;
- Regular back-ups of the data processed.

ANNEX B Subprocessors involved

Name	Services provided	Location
CJ2 Hosting B.V.	Cloud hosting provider	the Netherlands
Zapier, Inc.	App-to-app integration to allow Controller to connect third-party tools to Processor's platform	the United States