Data Protection Agreement

Alkmaar, January 13, 2022

THE UNDERSIGNED:

IB (ImpactBuying) B.V., a company incorporated under the laws of the Netherlands, having its registered office in (1812 RL) Alkmaar at the Toermalijnstraat 18 B, the Netherlands, hereinafter referred to as "IB", duly represented by Leontien Hasselman-Plugge, CEO;

(2) CUSTOMER

IB and Customer will collectively be referred to as "Parties", or separately as "Party";

WHEREAS:

a. Parties have concluded the Agreement, relating to the provision of services provided by IB to Customer;
b. In the context of the performance of the Agreement, Parties process Personal Data for which they qualify as either joint controllers or independent controllers in accordance with the Applicable Law, meaning that the Parties (jointly) determine the purposes and the means of the processing of the Personal Data;
c. With respect to the Processing Activities for which Parties qualify as joint controllers, Parties will have to make arrangements as to the processing of the Personal Data reflecting their respective roles and responsibilities for compliance with the Applicable Law, in particular as regards their respective responsibilities vis-à-vis each other and their respective roles and duties vis-à-vis the Data Subjects, among which their information duties and the exercising of the rights of Data Subjects;
d. In this Controller-Controller Data Protection Agreement, Parties wish to lay down their arrangements relating to the processing of the Personal Data in the context of the Agreement in accordance with the Applicable Law. This Controller-Controller Data Protection Agreement complements and forms an annex to the Agreement.

HAVE AGREED AS FOLLOWS:

1. DEFINITIONS

Non-capitalized terms not defined herein that are defined under the Applicable Law, such as processing, controller, processor, shall have the same meaning as meant under such the Applicable Law. All definitions included in the Agreement shall also apply to this Controller-Controller Data Protection Agreement, unless stipulated otherwise in this Controller-Controller Data Protection Agreement. In addition, thereto the following definitions apply to this Controller-Controller Data Protection Agreement.

a. 'Applicable Law' the law(s) or any other (local) regulations, guidelines or policies, instructions or recommendations of any competent governmental authority applicable to the processing of the Personal Data, including any amendments, replacements, updates or other later versions thereof;

b. 'Controller-Controller Data Protection Agreement' this Controller-Controller Data Protection Agreement, including its recitals and Schedules thereto, and any alteration, substitution, update or later versions thereof;

c. 'Data Breach' any event leading to (potential) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data transmitted, stored or otherwise processed, including where such destruction, loss, alteration, disclosure or access to the Personal Data cannot reasonably be ruled out;

d. 'Data Subject' the person to whom the Personal Data relate;

e. 'Employees' the employees and other persons engaged by a Party for the performance of the Agreement, who fall under the responsibility of such Party;

f. 'Personal Data' any data relating to an identified or identifiable living natural person, as meant under the Applicable Law, processed by a Party or its contractors in relation to the execution of the Agreement;

g. 'Processing Activities' the processing activities of Personal Data (to be) performed by the relevant Party in relation to the execution of the Agreement;

h. 'Agreement' the agreement between Parties dated based on which each Party performs its Processing Activities, including its recitals and annexes, and any updates thereof;

i. 'Schedule' attachment to the Controller-Controller Data Protection Agreement, which forms part of the Controller-Controller Data Protection Agreement;

j. 'Third Country' country that does not provide an adequate level of data protection according to the Applicable Law.

2. SUBJECT

a. In connection with the execution of the Agreement, each Party shall be the controller for the processing of Personal Data and qualify as (joint) controllers as set forth in the Applicable Law.

b. Each Party shall process the Personal Data in accordance with the Applicable Law. Parties shall make available to each other all information reasonably necessary to demonstrate compliance with the relevant requirements under the Applicable Law.

c. This Controller-Controller Data Protection Agreement complements and forms an annex to the Agreement and sets aside any (oral and/or written) arrangements of an earlier date relating to the processing of the Personal Data between Parties acting as controllers, in respect of the Personal Data, if applicable.

d. In case of any discrepancies between the provisions of this Controller-Controller Data Protection Agreement and/or the body of the Agreement, including any annexes thereto other than this Controller-Controller Data Protection Agreement, the provisions of this Controller-Controller Data Protection Agreement shall prevail, unless explicitly stipulated otherwise in this Controller-Controller Data Protection Agreement.

3. PROCESSING OF THE PERSONAL DATA

a. Schedule A to this Controller-Controller Data Protection Agreement contains a description of the Processing Activities performed by each Party and their respective roles vis-à-vis each other and roles and responsibilities vis-à-vis the Data Subjects.

b. In line with the Processing Activities as described in Schedule A, Parties shall maintain an adequately protected written or electronic record of all categories of Processing Activities carried out in line with the Applicable Law.

c. Taking into account the nature of the processing and the information available to each Party, Parties shall assist each other in ensuring compliance with the obligations that rest upon the Parties under the Applicable Law, more in particular the obligations in relation to the security of Personal Data, data protection by design and by default requirements, Data Breach notification and documentation duties, and the execution of data protection impact assessments, including prior consultation of a competent governmental authority.

d. Parties shall solely disclose the Personal Data to those Employees and/or contractors who necessarily need (access to) the Personal Data for the performance of the obligations of each Party under the Agreement, and for the remainder keep confidential, unless otherwise required under the Applicable Law.

e. Parties shall impose the obligations laid down in this Controller-Controller Data Protection Agreement and the Agreement, including the security and confidentiality obligations, to their Employees and/or contractors engaged by them to the extent these Employees and/or contractors are not bound by an appropriate statutory confidentiality obligation. Parties shall ensure that these Employees and/or contractors engaged by them, comply with these obligations.

4. CONTRACTOR

a. If a contractor acting as processor under the Applicable Law has been engaged for the processing of the Personal Data by a Party (also on behalf of the other Party) or by both Parties jointly, the relevant Party/Parties, shall conclude and enforce a written data processing agreement with such data processor in line with the requirements under the Applicable Law

5. SECURITY MEASURES

a. Parties shall implement appropriate technical and organizational security measures to ensure an appropriate level of security in relation to the Personal Data, in accordance with the Applicable Law, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

b. Parties shall regularly review their technical and organizational security measures, and update them where necessary.

6. REPORTING ON DATA BREACHES

a. Parties shall maintain adequate procedures designed to detect and respond to any Data Breaches, including procedures for preventive and corrective actions, and also to avoid recurrence of any Data Breaches. These procedures have been established in such a manner that both Parties will be able to meet their notification and documentation duties in relation to Data Breaches under the Applicable Law.

b. As soon as a Party detects a Data Breach or reasonably suspects that there has been a Data Breach related to the Processing Activities for which Parties are joint controllers, it shall notify the other Party as soon as possible and in any case within 24 hours upon detection or suspicion of the Data Breach.

c. Upon discovery or reasonable suspicion of a Data Breach as referred to in article 6.2 of this Controller-Controller Data Protection Agreement, Parties shall take adequate recovery measures without any undue delay.

d. Parties shall provide each other with all reasonable assistance and shall share with each other all necessary or by the other Party requested information, so that either Party will be able to notify, if applicable, the Data Subject(s) that was (were) (possibly) affected by the Data Breach as referred to in article 6.b of this Controller-Controller Data Protection Agreement, and/or the competent governmental authority/authorities, of the Data Breach in a timely manner and to prove compliance with their Data Breach notification duties in accordance with the Applicable Law. Parties shall enable each other to prove compliance with the Applicable Law in relation to either Party's Data Breach notification duties. Parties will consult each other on how and when the Data Subjects will be notified in a timely manner, if applicable, in accordance with the Applicable Law.

7. TRANSFER OF THE PERSONAL DATA

a. Parties shall fully cooperate at all times so that all requirements under the Applicable Law will be met to legitimize any transfer to a Third Country, from which follows that an adequate level of data protection is safeguarded in such jurisdiction.

b. If and to the extent Personal Data are transferred from IB to (an establishment of) Customer located in a Third Country, the unchanged EU-recommended controller-to-controller standard contractual clauses (Decision 2004/915/EC), or any updated version or replacement thereof, shall be deemed incorporated by reference herein and apply between IB as the data exporter and the Customer as the data importer.

c. Unless otherwise agreed by Parties, the standard contractual clauses referenced in clause 7.b of this Data Protection Agreement shall be governed by the Applicable Law of the EEA member state in which IB, as the data exporter, has its relevant establishment in relation to the processing of the Personal Data. IB shall be deemed to be the data exporter and Customer the data importer, and Schedule A of this Controller-Controller Data Protection Agreement shall be deemed to be the appendices of the applicable standard contractual clauses.

d. Prior to any transfer of Personal Data, the relevant data exporter in cooperation with the data importer shall carry out a legal assessment to determine whether the law or practice of the Third Country concerned, may undermine the effectiveness of the standard contractual clauses in the context of the specific transfer and shall identify and adopt supplementary measures, as they are required to provide a standard of protection for the Personal Data that is essentially equivalent to the level of data protection under the Applicable Law. If no essentially equivalent level of protection can be guaranteed, the data transfer will not take place. If the data transfer has already taken place, the Personal Data will be returned to the data exporter or deleted by the data importer.

e. The transfer of Personal Data to a third party located in a Third Country, shall, if required and no alternative data transfer mechanism applies legitimizing such transfer of Personal Data, be on the basis of the appropriate EU-approved standard contractual clauses (or any updated or replacing versions thereof). The appropriate standard contractual clauses shall be agreed by the relevant Party that has a (contractual) relationship with the third party, as data exporter, and the third party itself, as data importer.

f. Nothing in the Agreement or this Controller-Controller Data Protection Agreement shall be construed to prevail over any conflicting clause of the standard contractual clauses.

8. INFORMATION DUTIES TOWARDS DATA SUBJECTS AND RIGHT OF THE SUBJECTS

a. In so far Parties are joint controllers, Parties have determined their roles and responsibilities vis-à-vis the Data Subjects as laid down in Schedule A.

b. Parties shall fully cooperate with each other so that both Parties can live up to their obligations under the Applicable Law as (joint) controller if a Data Subject exercises its rights under the Applicable Law.

c. Parties acknowledge that irrespective of the terms of the Controller-Controller Data Protection Agreement, the Data Subjects may not be deprived to exercise their rights under the Applicable Law towards Parties.

9. INDEMNITY

a. Customer shall indemnify IB against any claim by a third party, including by any of the Data Subjects, imposed against IB as a result of a breach of the Applicable Law, which can be attributed to Customer or any of its Employees or any contractors engaged by Customer.

10. TERM AND TERMINATION

a. This Controller-Controller Data Protection Agreement enters into force on the date that Parties first process the Personal Data for the performance of the Agreement.

b. This Controller-Controller Data Protection Agreement shall remain in effect for the duration of the Agreement. In the event the Agreement ends, this Controller-Controller Data Protection Agreement ends as well by operation of law, without further legal action. Early termination of this Controller-Controller Data Protection Agreement by either Party is not possible.

c. If the Processing Activities of both Parties are inextricably linked, each Party, upon termination of the Agreement, shall safeguard that no irregularities or Processing Activities to the detriment of the Data Subjects shall come to pass.

d. Any obligation arising from this Controller-Controller Data Protection Agreement that by nature has post-contractual effect shall continue to be in effect after the termination of this Controller-Controller Data Protection Agreement.

Data Protection Agreement

Alkmaar, January 13, 2022

Schedule A

Overview of the Processing Activities,
insofar as relevant and applicable between IB and Customer

Purposes of the Processing Activities	Duration of the Processing Activities *Maximum and minimum retention periods*	Categories of Data Subjects	(Types of) Personal Data processed by the relevant Party or Parties *Where applicable differentiated based on sensitivity*	The role of the Parties and their respective duties towards governmental authorities and Data Subjects
IB processes certain personal data of authorized users / Employees of Customer (e.g. when they set up their User Account) in order to provide their cloud-based software solutions to Customer ("Services in general")	Same as Agreement	Authorized users / Employees of Customer	- Name and surname - Address - E-mail address - Phone number - Function title - Company name - Country - Password to User Account - IP address - Performance of your network and device - Type of your device - Language preferences - Operating system	Role of the parties: IB: independent controller Customer: independent controller Respective duties: As both Parties qualify as independent controllers, Parties are separately responsible for fulfilling their own GDPR duties as controllers towards governmental authorities and Data Subjects.

			- Information regarding the time and data when various requests are made - Login information - Preferences regarding information, news and other content - Statistics and information regarding user behaviour	
IB processes certain Personal Data of data subjects in the supply chain of Customer in order to provide "Advisory, Training and Consulting Services" and "IB Insights" to Customer	Same as Agreement	Contact persons working for parties that form part of the supply chain of Customer (and that might become Customer of IB in the future)	- Name and surname - Address - E-mail address - Phone number - Function title - Company name - Country	Role of the parties: IB: independent controller Customer: independent controller Respective duties: As both Parties qualify as independent controllers, Parties are separately responsible for fulfilling their own GDPR duties as controllers towards governmental authorities and Data Subjects.
IB and Customer process certain Personal Data of the data subjects in the supply chain of Customer so that supply chain data on the Platform of IB's SaaS service can be structured ("SaaS service") and IB and Customer gain more insight in the supply chain data concerned ("Data Solutions")	Same as Agreement	Contact persons / data subjects working for parties that form part of the supply chain of Customer (and that might become Customer of IB in the future itself)	- Name and surname - Address - E-mail address - Phone number - Function title - Company name - Country	Role of the parties: IB and Customer: joint controllers Respective duties: 1. Data Breach notification requirements to governmental authorities and/or data subjects: Customer will notify the competent governmental authority and/or the Data Subjects.

				2. **Information duties for the processing of Personal Data towards Data Subjects: Customer will inform the Data Subjects.** 3. **Handling requests from Data Subjects: IB will handle the Data Subjects' requests.**