Data Processing Agreement

THE PARTIES:

IDH Sustainable Trade Initiative, a foundation incorporated under the laws of the Netherlands, having its registered office at Arthur van Schendelstraat 500 (3511 MH) Utrecht, the Netherlands, registered at the Dutch Chamber of Commerce under number 53521129 (hereinafter referred to as "**Data Controller**"); and

[DATA PROCESSOR], incorporated and registered in [COUNTRY] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS], registered [at the Dutch Chamber of Commerce ("*Kamer van Koophandel*")] under number [NUMBER] (hereinafter referred to as "**Data Processor**").

Data Controller and Data Processor, each a "**Party**" and together referred to as the **"Parties"**.

WHEREAS:

A. On [INSERT DATE], the Parties concluded an agreement under which Data Processor will conduct [DESCRIPTION SERVICES] (the "**Agreement**");

B. Under the Agreement, Data Processor will, on behalf of Data Controller, [SERVICES] and process Personal Data (as defined hereafter).

C. Under article 28 of the General Data Protection Regulation, the Parties are required to conclude a data processing agreement;

D. The Parties will enter into this data processing agreement ("**Data Processing Agreement**") in order to fulfill their obligations under the General Data Protection Regulation.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS

1.1. The following terms as used in this Data Processing Agreement shall, unless the context clearly indicates to the contrary, have the meanings set forth in this Clause:

"**Agreement**"	means the agreement referred to in recital A hereto;
"**Applicable Laws**"	means all laws and legislation, including the GDPR and the Dutch Implementation Act relating to the GDPR (*Uitvoeringswet AVG*), that are applicable to the

	Processing of Personal Data by the Data Controller and the Data Processor under the Agreement;
"**Data Breach**"	means any breach of security of Personal Data;
"Data Processing Agreement" or "DPA"	means the present data processing agreement including the annexes hereto;
"GDPR"	means the General Data Protection Regulation (EU) 2016/679;
"**Personal Data**"	means any information relating to an identified or identifiable natural person, obtained in relation to the Agreement, as set out in **ANNEX 1**;
"**Processing" or "Process**"	means any operation or set of operations which is performed on Personal Data, whether or not by automatic means, as set out in article 4 of the GDPR;
"**Sub Processor**"	means any processor, as defined in the GDPR, engaged by the Data Processor and any processor engaged by the processor who agrees to Process Personal Data on behalf of the Data Controller; and
"**Technical and Organizational Measures**"	means the technical and organizational measures as defined in the GDPR.

2. OBLIGATIONS OF THE DATA PROCESSOR

2.1. The Data Processor shall:

a. Process Personal Data in accordance with Applicable Laws;

b. not Process any Personal Data other than in accordance with the Data Controller's instructions as set out in the Agreement;

c. only store the Personal Data for as long as the Data Controller requires and correct, anonymize, block or delete the relevant Personal Data at the Data Controller's instructions; and

d. ensure that the only persons able to process or access any particular Personal Data in Data Processor's or Sub Processor's possession, custody or control in the performance of the Agreement are (i) the Data Processor's employees or (ii) Sub Processor's employees

who need to process or access such Personal Data in order to carry out their duties in connection with the Agreement.

3. TECHNICAL AND ORGANIZATIONAL MEASURES

3.1. The Data Processor shall:

a. adopt and maintain appropriate Technical and Organizational Measures. Such Technical and Organizational Measures will at least include the Technical and Organizational Measures as set out in **ANNEX 2;**

b. taken into account the nature of the processing as well as with all the means at its disposal provide the Data Controller assistance in ensuring compliance with regard to the obligations arising from Applicable Laws, especially articles 32 up to and including 36 of the GDPR.

3.2. The Data Processor ensures that the Technical and Organizational Measures as mentioned in paragraph 3.1 are:

a. appropriate, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of persons, that, where appropriate, may include, but are not limited to:

i. the pseudonymization and encryption of personal data;
ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
iii. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
iv. a process for regularly testing, assessing and evaluating the effectiveness of Technical and Organizational Measures for ensuring the security of the processing.

b. adopted and applied in such a way that the Data Controller, with regard to the processing that is entrusted to the Data Processor, constantly acts in compliance with the Applicable Laws.

3.3. The Data Controller has the right to instruct the Data Processor to take additional security measures. The Data Processor shall implement these additional security measures within a reasonable time.

4. USE OF SUB PROCESSORS

4.1. The Data Processor may not engage a Sub Processor, unless the Data Processor:

a. obtains prior written consent of the Data Controller; and

b. enters into data processing agreements with the relevant Sub Processors which requires the Sub Processor to abide by the same obligations as the Data Processor under this Data Processing Agreement.

4.2. In relation to the Data Controller, the Data Processor is fully responsible for the fulfilment of the obligations of the Data Processing Agreement by the Sub Processor.

5. TRANSFER OF PERSONAL DATA

5.1. The Data Processor may only transfer and Process Personal Data in a country outside the Netherlands, if Data Processor acts in accordance with local applicable law and regulations on Processing of Personal Data.

5.2. The Data Processor may not transfer Personal Data to a country outside the European Economic Area ("**EEA**"), unless the Data Controller instructs the Data Processor in writing prior to the transfer or the Data Processor is obliged to transfer Personal Data on the basis of a statutory provision. In case a statutory provision requires the Data Processor to transfer personal data outside the EEA, the Data Processor will prior to the transfer inform the Data Controller, unless the statutory provision due to overriding reasons of general interest prohibits the Data Processor from doing so.

5.3. If the Data Controller instructs the Data Processor to transfer personal data to a country outside the EEA the Data Processor is only permitted to transfer and process personal data to this country, in case:

a. such country offers an adequate level of protection according to the EU 'white list' of countries offering adequate data protection standards; or

b. EC Model Clauses are concluded between the Data Controller and the Data Processor or a Sub Processor, as set out under article 46, paragraph 2, sub paragraph c and d GDPR; or

c. the transfer is allowed based on another legal ground under Applicable Laws and the Data Controller has explicitly consented with a transfer based on such legal ground.

5.4. In case Personal Data is transferred to a Sub Processor located in a country outside the EEA and there are no EC Model Clauses as set out under paragraph 5.3 (b) available that regulates the transfer between two processors, the Data Controller hereby instructs and authorizes the Data Processor to instruct the Sub Processor in Data Controller's name and vis-a-vis the Sub Processor's to conclude EC Model Clauses.

6. AUDITS

6.1. The Data Controller or another auditor mandated by the Data Controller is at any given moment entitled to audit Data Processor's and its Sub Processor's compliance with this Data Processing Agreement and more specifically with respect to the Technical and Organizational Measures.

6.2. The Data Processor shall provide the Data Controller and its auditors with all reasonable cooperation, access to its Processing facilities and assistance in relation to each audit and shall ensure that its Sub Processor's will do the same.

6.3. The Data Processor will cover its own as well as the Data Controller's expenses in connection with any such audit in the event that the Data Processor breaches this Data Processing Agreement.

7. CONFIDENTIALITY

7.1. The Data Processor keeps all Personal Data strictly confidential and ensures, prior to the disclosure of Personal Data to its employees, Sub Processors or employees of Sub Processors, that these persons are bound by the same conditions of confidentiality.

7.2. Subject to Clause 7, the Data Processor may disclose Personal Data when a law requires the Data Processor to disclose Personal Data or when the Data Controller instructs the disclosure of Personal Data.

7.3. When a Data Processor has reasonable doubts as to whether the Data Processor is permitted to disclose information, Data Processor shall consult with Data Controller.

7.4. The obligation of confidentiality shall also apply after termination of this Data Processing Agreement.

8. NOTIFICATION OF A DATA BREACH

8.1. As part of the obligations incumbent on the Data Processor with regard to the security of personal data, the Data Processor shall establish and maintain procedures designed to reasonably detected Data Breaches and then implement the correct measures, including recovery measures.

8.2. The Data Processor will promptly, as soon as possible under the circumstances, notify the Data Controller, as set out in Clause 8.3, about (i) any legally binding request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, and (ii) a Data Breach.

8.3. The Data Processor will notify the Data Controller about every Data Breach as well as:

a. the start and end time and date and the location of such event;
b. the nature and scale of such event;
c. the department or part of the system in which the event occurred;
d. the time needed to reverse damage of the Data Breach;
e. the nature and scope of Personal Data records concerned;
f. the categories and approximate number of data subjects concerned;

g. the likely consequences of such event, including the consequences for the Data subject and a proposal to prevent damage and other negative consequences;
h. measures taken or to be taken to mitigate the consequences of the Data Breach; and
i. the name and contact details of the data protection officer or other contact point where more information about the Data Breach can be obtained.

8.4. The Data Processor will promptly, without delay, and in any case within 24 hours of discovery of a Data Breach notify, as set out under Clause 8.2 and 8.3, the Data Controller and subsequently keep the Data Controller fully informed about any progress of the recovery or other relevant developments with respect to such event.

8.5. The Data Processor shall without delay take all reasonable measures to recover the Personal Data and reduce the negative impact of a Data Breach. The Data Processor is obliged to inform Data Controller of these measures as soon as possible.

8.6. The Data Processor shall not, on its own initiative, notify data subjects that are affected or likely to be affected by a Data Breach or the supervisory authority that is competent to take notice of a Data Breach.

9. REQUESTS BY DATA SUBJECTS

9.1. The Data Processor will provide all reasonable assistance to ensure that the Data Controller is able to fulfil its legal obligations when a data subject exercises his or her rights under the Applicable Laws.

9.2. As soon as the Data Processor receives a request as mentioned in paragraph 9.1, the Data Processer shall promptly inform the Data Controller. The Data Processor shall not respond to the request without the consent of the Data Controller.

9.3. On the instruction of the Data Controller, the Data Processor shall, without delay, correct, erase or otherwise adjust or process the Personal Data.

9.4. The Data Processor will promptly inform the Data Controller about any request or complaint of the Data Subject with respect to the processing of its Personal Data.

10. LIABILITY

10.1. The Data Processor is liable for and indemnifies and hold the Data Controller harmless from and against all (i) damages; and (ii) fines imposed by regulators, which arise from or in connection with or the Data Processor’s failure to perform any one or more obligations under this Data Processing Agreement.

10.2. Data Controller's entire and aggregate liability under this Data Processing Agreement, irrespective of the grounds for liability including indemnities and breached warranties, for any

and all events will be limited to 50% of the fees paid to Data Processor under the Agreement in the twelve (12) months preceding the event giving rise to such liability.

10.3. Clause 10.2 is not applicable to liability arising in connection with (i) wilful default or (ii) gross negligence.

11. TERM AND TERMINATION

11.1. This Data Processing Agreement is concluded on the moment the Parties signed the same and is effective until termination or expiration of the Agreement.

11.2. Parties agree that on the day of termination of this Data Processing Agreement, the Data Processor shall, at the choice and the costs of the Data Processor return all Personal Data and the copies thereof, by means of the Data Controllers choice, to the Data Controller or a third party designated by the Data Controller.

11.3. After the return of the Personal Data, a written rejection of the return of the Personal Data by the Data Controller, or if the Data Controller does not respond within one month after the offer to return the data, the Data Processor will promptly destroy all Personal Data. On request of the Data Controller, the Data Processor will confirm to the Data Controller in writing that it has destroyed the Personal Data.

12. MISCELLANEOUS

12.1. This Data Processing Agreement shall be governed by, and construed in accordance with, the laws of the Netherlands.

12.2. No term of this Data Processing Agreement shall be amended or modified, unless such amendments or modifications are made in writing with express reference to this Data Processing Agreement and signed by both parties.

12.3. The Data Processer will accept any modification of this Data Processing Agreement which is incorporated for the purpose of compliance with Applicable Laws.

-signature page follows-

SIGNED BY THE PARTIES FOR AGREEMENT

For IDH	**For [NAME PARTY]**
_____	_____
Name: [Joost Oorthuizen/Céline Bouquet]	Name: [NAME SIGNATORY]
Position: **[**CEO/COO]	Position: **[**ADD POSITION]
Date: _____	Date: _____

Salesforce number

ANNEX 1

DESCRIPTION OF PROCESSING OPERATIONS

Categories of personal data

The Personal Data processed concern the following categories of data:

- Name
- Address
- Telephone number
- Gender
- Financial data
- Household data
- Geolocation data
- [and other data provided by the farmer in relation to the interviews and surveys]

Salesforce number

ANNEX 2

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES

This Annex describes the technical and organizational security measures and procedures that the Data Processor shall maintain to protect the security of Personal Data. The Data Processor will keep documentation of technical and organizational measures identified below to facilitate audits and for the conservation of evidence.

[Insert IT security measures implemented by Data Processor]

1)

1.1) Physical access control

- *Is the office secured? For example by limiting access through locks, electronic entrance passes for staff members, biometric authentication, alarm system (also for natural hazards), security staff members, camera surveillance, accompany visitors, extra secured rooms (like server rooms) and registration of access.*

1.2) Technical access control

- *How are the servers protected? For example secured network, firewall and other protection against malware etc, separated server.*
- *In what manner are the computers protected? For example login name and password, secured transmission of authentication data, monitoring of online access (via web application e.g.)*
- *How is access to Personal Data secured? For example access based on the roles/authorised groups within software programs, document of roles and authorisations, registration of access, changeover possibilities, periodic back ups and an emergency plan.*

2) Management of the lifecycle of data

2.1) Enter data

- *In what way is it allowed to process Personal Data? For example determining purposes of processing, defining the use of Personal Data (read-only mode, blocking of data transfers, etc.), processing by trained professionals and closing of a non-disclosure agreement.*
- *How is the data processing being controlled? For example determining input, authorising input and checking of processing purposes.*

2.2) Security and storage of Personal Data

- *How is Personal Data protected? For example: encryption/pseudonymisation/anonymization of databases, transfer of devices, blocked entrance for USB's or similar devices, separation from processing activities, revised and testing of security measures.*
- *For what period of time can Personal Data be stored and how is it destroyed? For example automatized erasure, secured erasure and destruction, control of data minimisation and storage periods, erasure from a distance when devices are involved.*

3) Exchange of Personal Data

- *Who is allowed to receive or send Personal Data? For example determine safe receivers or*

senders, record data transfers.

- *How is the exchange of Personal Data secured? Secured transfer of Personal data (via encryption), secured network, machinery to machinery authentication, digital signature, documents secured with passwords.*

4) Control

- *How are Technical and Organisational Measures, as they are named here, checked and evaluated? For example via an external or internal audit, periodic execution of a data protection impact assessment, appointment of a Data Protection Officer.*

ANNEX 3

DESCRIPTION OF SUB PROCESSORS

With prior consent of the Data Controller, the Data Processor engages the following Sub Processors:

- [INSERT]

Salesforce number