Data Processing Agreement [*Verwerkersovereenkomst*]
FMO

Contents:

Date: 14 June 2018

Contract number: [enter].

The undersigned:

Nederlandse Financierings-Maatschappij voor Ontwikkelingslanden N.V. (a company incorporated in The Netherlands, registered number 27078545), whose registered office is at Anna van Saksenlaan 71, The Hague 2593 HW, The Netherlands ("FMO");

and

[Name company] (a company incorporated in [Name country] registered number [number]) whose registered office is at [street name, and number], [city, postal code], [country] (the "Processor").

FMO and Processor shall hereinafter be jointly referred to as 'Parties';

WHEREAS:

- FMO concluded an Agreement bearing reference [enter] with the Processor on [date] regarding the performance of work in the field of [enter] (to be referred to hereinafter as: the "Agreement");
- Said performance will involve the processing of Personal Data as defined in Section 4(1) EU General Data Protection Regulation (to be referred to hereinafter as: the "GDPR");
- Pursuant to the provisions of Section 1 GDPR, FMO will be the Party responsible for the processing of this Personal Data, while the Processor will act as the Processor;
- The GDPR requires FMO to create clear and strict guidelines regarding the processing of personal data by a processor.
- In accordance with the GDPR, the Parties wish to lay down their agreements regarding the Processor's processing of Personal Data as the Processor in this Data Processing Agreement;
- This Data Processing Agreement is to be considered a processing agreement as defined in Section 28(3) GDPR.

AGREE AS FOLLOWS:

1. Terms

The terms written in capital letters in this Data Processing Agreement are defined as follows:

1.1 Personal Data: all data relating to an identified or identifiable natural person;

1.2 Processing: an action or totality of actions regarding Personal Data, including in any case the collection, recording, structuring, storage, updating, alteration, retrieval, review, or use of said data, the provision of said data by forwarding, dispersing, or otherwise making it available, and the combination or association of said data, as well as the partitioning, deletion, or destruction of said data.

1.3 Agreement: the Agreement between FMO and [enter] of [date] regarding [enter].

1.4 Data Processing Agreement: the present agreement, including the recitations and accompanying appendices.

1.5 Relevant Party: the person to whom the personal Data relates.

1.6 Security Incident: a breach of security of the personal Data, as defined in Sections 33 GDPR, being processed by the Processor in the context of this Data Processing Agreement.

1.7 Data Breach: a breach of security as defined in Section 33 GDPR which leads to a substantial risk of severe negative consequences or which has serious negative consequences for the protection of personal Data.

2. Effective Date, Term, and Termination of the Data Processing Agreement

2.1 This Data Processing Agreement will not enter into effect before the date on which the Parties' Agreement relating to this Data Processing Agreement enters into effect.

2.2 This Data Processing Agreement will remain in effect throughout the term of the Agreement. If the Agreement is terminated, this Data Processing Agreement will terminate by operation of law unless the nature of the processing or the nature of the provision demands that specific provisions of this Data Processing Agreement remain in effect.

2.3 Neither of the parties may terminate this Data Processing Agreement prematurely.

3. Subject of the Data Processing Agreement

3.1 The Processor will, at the order of FMO, process the personal data described in Appendix 1 which FMO has collected under its responsibility as described in that same appendix.

3.2 The Processor will process the personal data properly and carefully and in accordance with the GDPR and other applicable laws and regulations regarding the Processing of personal data.

3.3 The Processor will only process personal data on the order of FMO and will follow all of FMO's instructions in this respect unless doing do would violate statutory obligations.

3.4 The Processor has no control regarding the object and means for processing personal data. To the extent not stipulated otherwise in this Data Processing Agreement, the Processor will not take any decisions regarding the use of the personal data, its provision to third parties, or the length of time for which the personal data will be stored.

3.5a The Processor will not engage any third parties ("Sub-Processors") to perform the Processing without notifying FMO of that fact in writing at least four weeks in advance. If FMO has serious objections, it shall notify the Processor of those objections as soon as possible and the Parties will enter into negotiations to arrive

at an alternative solution. Unless it has obtained prior consent, the Processor is not permitted to engage Sub-Processors if this would result in personal data being Processed outside the European Economic Area (EEA). FMO may attach additional conditions to its consent to the engagement of third parties.

3.5b If the Processor engages a Sub-Processor, the Processor will conclude written agreements with the Sub-Processor as laid down in this Data Processing Agreement. The Processor will remain responsible for the Sub-Processor's performance of the stipulations laid down in this Data Processing Agreement.

3.6 The Processor is not permitted to provide personal data to any party other than FMO, unless it does so pursuant to the FMO's written request or with the latter's consent. The Processor is obliged to confirm in writing that such provision has been made, in which respect it must provide an exact description of the personal data provided, the Relevant Party (or Relevant Parties), the recipient(s), and the date and time of the provision.

3.7 If the Processor must provide data pursuant to a statutory obligation, the Processor will verify the basis for the request and the identity of the requesting party, and it will notify FMO immediately, if possible prior to the provision. The Processor is obliged to confirm in writing that such provision has been made, in which respect it must provide an exact description of the personal data provided, the Relevant Party (or Relevant Parties), the recipient(s), and the date and time at which the data was provided.

3.8 The Processor will lend FMO its full cooperation to meet the statutory deadlines for meeting obligations pursuant to the GDPR, more particularly the rights of Relevant Parties, including, but not limited to, a request to examine, correct, supplement, remove, or partition personal Data and the implementation of an objection that has been filed and sustained.

3.9 If the Processor determines that a Security Incident has occurred, it will notify FMO of that fact immediately – but within no more than 24 hours – and it will take all measures that are reasonably necessary to terminate, prevent, or mitigate the Security Incident and other unlawful Processing or breaches, all of this without prejudice to the Processor's potential obligation to pay FMO damages for the resulting harm or loss.

3.10 After the Processor has notified FMO of a Security Incident as laid down in Clause 3.9, the Processor will keep FMO apprised of new developments relating to the Security Incident and the measures that the Processor has taken to limit the consequences of the Security Incident and prevent recurrence. The Processor will also lend the FMO its full cooperation with meeting its duty to report to the Dutch Data Protection Authority [*Autoriteit Persoonsgegevens*] and the Relevant Parties as required by Sections 33 and 34 GDPR. Stipulations regarding how the Processor will notify FMO are included in Appendix 2.

3.11 Any costs incurred in connection with Clauses 3.8 up to and including 3.10 will be borne by the party that has incurred said costs.

3.12 Without prejudice to the provisions of Section 82 GDPR, the Processor will be liable to an administrative penalty or a fine imposed by the Dutch Data Protection Authority, or for the harm or loss incurred by the Relevant Party (or Relevant Parties) or FMO as a result of a Processor's culpable failure to perform its obligations.

4. Applicable Terms and Conditions

To the extent not stipulated otherwise in this Data Processing Agreement, the provisions of the Agreement will apply to this Data Processing Agreement.

5. Continuing Obligations

The obligations of the Processor which, by their nature, must remain in effect after the expiry of the Agreement and the Data Processing Agreement, will remain in effect for an indefinite term. This scope of this clause in any case includes – but is not limited to – transfers, the identification of unauthorised Processing and confidentiality, and indemnification, as laid down in more detail in Clauses 3.8, 3.9, 3.10, 3.12, 6, 9.4, and 11.

6. Return of Personal Data

After the expiry of the Agreement and the Data Processing Agreement, all personal data, copies and processed versions thereof, as well as all data carriers on which the personal data, copies and processed versions thereof have been or will be stored, must be returned and/or provided to FMO (or a third party it designates) immediately upon its first request, or must be destroyed, all at FMO's discretion. If FMO does not expressly request the personal data to be destroyed, the Processor will destroy the personal data on its own initiative after the expiry of the agreed retention term referred to in Appendix 1. Moreover, upon the termination of this Data Processing Agreement, the Processor will lend its full cooperation regarding the transfer of the work regarding the Processing of the Personal Data to FMO or a subsequent Processor and will do so in such a way that will safeguard the continuity of the service as much as possible from the moment at which the transfer takes place. To the extent such costs are not included in the Processor's agreed prices and fees relating to the performance of the Agreement, the costs the Processor incurs in making these efforts will be borne by FMO.

7. Intellectual Property Rights

All intellectual property rights – including copyrights and database rights – relating to the collection of Personal Data, copies or processed versions thereof, will at all times accrue to FMO or its licensor(s).

8. Security

8.1 The Processor will implement technical and organisational security measures with regard to the Processing of the personal data. These measures will, with due observance of the state of the art and the costs involved in implementing and executing the measures, ensure an appropriate level of security, taking into account the risks inherent in the Processing of personal data and the nature thereof.

8.1a The Processor has in any case taken the following measures [*please check measures also to be in accordance with FMO's policy*]:

- Logical access control, use of strong passwords;
- Physical measures for access security;

- Adequate encryption of digital files containing personal data, based on the nature of the personal data;
- Organisational measures for access security;
- Securing network connections via Secure Socket Layer (SSL) technology;
- A secured internal network;
- Warranting the integrity and availability of the personal data;
- Warranting that personal data will be recoverable in the event of physical or technical Security Incidents;
- Regular evaluation and testing of security measures;
- Automatic logging of access to personal data;
- Adequate reporting on the control of authorisations granted and the processing of personal data in line with the requirements of this provision.

8.1b The Processor will establish and implement a security policy regarding the processing of FMO's personal data. Said policy will note the vulnerabilities of the relevant system and/or system(s) and describe the measures to be taken to monitor these and to prevent, limit, and eliminate risks.

8.2 The Processor will not process personal data outside a Member State of the European Union and the European Economic Area (EEA) unless it obtains FMO's express written consent.

9. Confidentiality

9.1 The Processor is bound by a duty of confidentiality in respect of all personal data that it processes in relation to this Data Processing Agreement.

9.2 If and to the extent FMO expressly so requests in writing, the Processor will take special measures regarding the personal data referred to in the request in order to ensure that it is kept confidential, which measures could include destroying the relevant personal data as soon as the Processor no longer requires it.

9.3 The Processor will include clauses in its agreements with its employees that will impose on those persons the same duty of confidentiality as that imposed by Clauses 9.1 and 9.2 with regard to all personal data which they Process by virtue of their employment by the Processor. The Processor warrants to FMO that the relevant persons will comply with said clauses.

9.4 The obligations pursuant to this Clause 9 will remain in effect after the expiry of the Agreement and this Data Processing Agreement.

10. Auditing

10.1 Once per year, by no later than 31 December, the Processor will provide to FMO:

- a statement by its duly authorised representative of that individual's assessment of the performance of this Data Processing Agreement.

- an overview of the measures taken by the Processor regarding technical and organisational security measures and any points meriting attention in this regard. If the Processor intends to change the technical and organisational security measures that have been taken, the Processor will report this to the FMO as soon as a proposal for this resolution has been prepared.

10.2 If FMO suspects that the Processor is not performing its obligations pursuant to this Data Processing Agreement, FMO may, at any time, audit the Processor's Processing and its compliance with the agreed technical and organisational security measures (or the Processing and compliance with the agreed technical and organisational security measures performed by any Sub-Processor(s) engaged by the Processor), or may cause same to be audited, as well as said parties' compliance with the measures referred to in Appendix 2 which are required to satisfy the duty to report referred to in Sections 33 and 34 GDPR.

The Processor will lend all reasonably required cooperation to said audit and will ensure that the Sub-Processor(s) it has engaged lend all reasonably required cooperation to said audit.

10.3 The performance of an audit will not result in a delay of the work to be performed by the Processor in the context of the Agreement and this Data Processing Agreement. Should that unexpectedly be the case, the Parties will enter into negotiations to arrive at a solution as quickly as possible.

10.4 The costs associated with the audit will be borne by FMO unless the audit shows that the Processor or Sub-Processor has failed to perform its obligation(s) pursuant to this Data Processing Agreement and/or the Agreement.

10.5 The Processor will follow the recommendations made by FMO within the term FMO sets for same.

11. Indemnification

The Processor will indemnify FMO against all third-party claims against FMO and for all loss or harm or expenses that FMO incurs as the direct or indirect result of the Processor's violation of its obligations pursuant to this Data Processing Agreement.

12. Penalty

In addition to the provisions on liability agreed in other terms and conditions that apply to the relationship between FMO and the Processor, the Processor will forfeit a penalty of EUR 250,000 to FMO for each event involving a violation by the Processor, its staff, or any Sub-Processors, of any duty it has/they have pursuant to this Data Processing Agreement.

13. Final provisions

13.1 Deviations from this Data Processing Agreement will only be binding to the extent they are expressly agreed between the Parties in writing.

13.2 General terms and conditions of supply or any other general or special terms and conditions applied by the Processor will not apply to this Data Processing Agreement, and FMO expressly rejects any such terms or conditions.

13.3 This Data Processing Agreement is a supplement to the Agreement. Should any provisions of this Data Processing Agreement conflict with provisions of the Agreement, the provisions of this Data Processing Agreement will prevail.

Thus agreed and signed in duplicate original on the later of the two dates referred to below,

The Hague, [date]	[City/town], [date]
FMO	[name of Processor]
by, [job title of signatory]	
[job title of signatory]	[name and job title of signatory]

Appendix 1. The processing of personal data (Clause 3.1)

This Appendix must include more details about at least the following:

- Describe the activities in the context of which personal data will be processed, possibly with reference to the Agreement:

- Describe which personal data of which Relevant Parties is involved:

- Describe what processing will be done, including, as appropriate, the Processor's processing of personal data, transporting of personal data, storage of personal data, and making of a back-up:

- Describe the purpose or purposes for which the personal data is processed:

- Describe the categories of Relevant parties, data subjects, of which personal data will be processed:

- Describe how long personal data must be retained:

- Indicate whether one of the following types of data will be processed and, if so, which:
  - Race
  - Sexual orientation
  - Membership of a trade union
  - Religion or personal belief
  - Political preference
  - Criminal history information;
  - Medical information
  - Biometric information

- Indicate the country in which the personal data will be processed (Note: This can also be the country from which the Processor has access to the personal data);

Appendix 2: Measures in connection with the duty to report data breaches (Clause 3.9)

1. The Processor will notify FMO immediately of any Security Incident, based on which FMO can establish whether it is required to report this Security Incident immediately to the Dutch Personal Data Authority as a Data Breach as defined in Sections 33 and 34 GDPR or to notify the Relevant Party or Relevant Parties.

2. The Processor will inform FMO within 12 hours after a Security Incident is discovered by the Processor or the Sub-Processor(s) or third parties it has engaged. This obligation to notify FMO will apply at all and any times, without any restriction (24 hours/seven days a week).

3. FMO must be notified about the Security Incident by sending the information below by e-mail to: [email]@fmo.nl; a.singh@fmo.nl; m.rocker@fmo.nl.

4. The information to be provided consists of the notification of the fact that a Security Incident has occurred. If, based on the information provided by the Processor, FMO establishes that the Security Incident qualifies as a Data Breach, the information below will also be provided:

- A summary of the events relating to the Data Breach.
- Indicate whether the Data Breach occurred at the Processor or at a Sub-Processor and, to the extent relevant, the identity of this Sub-Processor.
- The date and time, or period within which, the Data Breach was discovered and occurred.
- Indicate the cause (or suspected cause) of the Data Breach.
- Characterise the Data Breach based on the following options: reading, copying, altering, deleting, destroying, or theft of Personal Data.
- Describe the types of Relevant Parties, the minimum and maximum possible number of Relevant Parties, and, if known, the identity of these persons and the presence of Relevant Parties in other EU Member States.
- The categories of Personal Data that were (or may have been) affected by the Data Breach, such as: Name and address information, telephone numbers, e-mail or other addresses for electronic communication, access or identification information (such as login names, passwords, or customer numbers), financial data (such as account or credit card numbers), Citizens Service Numbers [*Burgerservicenummer* or *BSN*] or social security numbers [*sofinummer*], copies of passports or other proof of identity, gender, birth date and/or age, certain personal data (such as race, ethnicity, criminal background, political stance, trade union membership, religion, sexual orientation or practices, medical information), or other personal data;

- Indicate whether the Personal Data in question was in any way encrypted, anonymised, assigned pseudonyms, or hashed, or if it can be remotely deleted;

- Explain what the consequence (as far as known and/or expected) will be for persons whom the data concerns, such as: stigmatisation or exclusion, harm to health, exposure to fraud (including identity fraud), exposure to spam or phishing, or other;
- Describe the technical and organisational measures that have been, or will be, taken to mitigate the consequences of the Data Breach and prevent recurrence.
- Provide contact details for following up on the report and obtaining more information about the Data Breach.

5. The Processor must also, on its own initiative, inform FMO of all relevant developments relating to the Data Breach that occur after the time the information listed in Appendix 2 has been provided. The Processor must, within a reasonable period of time, respond to any additional questions FMO has about the Data Breach.

6. As soon as the Data Breach is discovered, the Processor must also, at its own risk and expense, take all measures that are reasonably necessary to mitigate all of the negative consequences of the Data Breach and to prevent recurrence.

7. The Processor will lend FMO all cooperation, and provide all information, that is reasonably necessary in order to enable the Dutch Data Protection Authority to inform each Relevant Party, individually, about the cause and magnitude of the Data Breach. If the circumstances so prompt, the Processor will permit FMO to access the system of the Processor and/or the Sub-Processors engaged by the Processor.

8. In addition to the forgoing, FMO reserves the right to ask for additional information related to the Data Breach when FMO considers it necessary to gather more information to comply with its own Data Breach notification requirements. After the notification as described in clause 2.1 above, the Processor shall endeavour to provide FMO with any relevant additional information on the Data Breach involving FMO Personal Data within twenty-four (24) hours or otherwise as soon as reasonably possible.

9. Processor shall maintain an inventory of Data Breaches, involving FMO Personal Data, comprising the facts surrounding each Data Breach, its effects and the remedial action taken. Processor shall ensure that said inventory shall be sufficient to enable the Dutch Data Protection Authority to verify compliance with the obligation to notify personal Data Breaches under the Applicable Law. Processor shall make this inventory available to FMO upon FMO's first request.

10. Processor shall cooperate with FMO and follow FMO's instructions to enable FMO to properly investigate, respond to or follow up on any Data Breach.

11. The Processor is not permitted to notify the Dutch Data Protection Authority or the Relevant Parties of the Data Breach itself.