Appendix 7

Agreement between Personal Data Controller and Personal Data Processor

Content

1 Parties

This Personal Data Processing Agreement was concluded by the parties on the date of the signatures:

1) Personal Data Controller:

   The Embassy of Sweden in Lusaka
   Haile Selassie Avenue
   Lusaka, Zambia

   (the “Controller” or “Sida”)

2) Personal Data Processor:

   [Name].
   [Corporate ID number].
   [Address].

   (the "Processor” or “Supplier”)

2 Background and purpose

2.1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter referred to as "Data Protection Regulation") requires that a written agreement be concluded when a legal or natural person will process personal data on behalf of a Personal Data Controller.

2.2 The Controller and the Processor have entered into an agreement [Dox-Document ID and name of contract with supplier]., hereinafter referred to as the "Main Agreement", under which the Supplier shall assist Sida with [insert a brief description of the nature of the assignment].. The assignment entails that the Supplier will process personal data on behalf of Sida.

2.3 In connection with this, the Parties now conclude this Personal Data Processing Agreement. This Agreement regulates the processing of personal data by the Processor in accordance with the Controller's instructions and applicable law, regulations and practices. The Agreement covers any processing of personal data performed by the Processor on behalf of the Controller within the boundaries of the purposes set out in Clause 4.2 of this Agreement.

2.4 To the extent that Data Protection Regulation contains concepts similar to those used in this Agreement, such concepts shall be interpreted and applied in accordance with the Data Protection Regulation.

3 Terms used in this Agreement

- *Data protection legislation* means privacy and personal data legislation as well as any other legislation (including rules and regulations) applicable to the processing of personal data under this Agreement.

- *Personal data controller* means a person who solely or jointly with others determines the purposes and means of processing personal data.

- *Personal data processor* means a person who processes personal data on behalf of the Personal Data Controller.

- *Personal data* means any information that can be directly or indirectly attributed to a natural person who is alive. Personal data in this Agreement also refers to information about deceased persons in relevant cases.

- *Processing of personal data* means a measure or a combination of measures concerning personal data or sets of personal data, whether or not they are automated, such as collection, registration, organisation, structuring, storage, adaptation or alteration, creation, reading, use, disclosure by transmission, dissemination or otherwise making available, adjustment or bringing together, limitation, deletion or destruction.

- *Personal data breach* means a security incident leading to accidental or unlawful destruction, loss or alteration or unauthorised disclosure of or access to the personal data transmitted, stored or otherwise processed.

- *Data subject* means the person to whom the personal data relates.

- *Third country* means a state which is not a member of the European Union or part of the European Economic Area.

4 Purpose and scope of personal data processing

4.1 The purpose and scope of the Processor's assignment on behalf of the Controller is set out in the Main Agreement.

The purpose of the processing

4.2 The Processor may process personal data on behalf of the controller to perform audit services relating to Sweden’s bilateral development cooperation with Zambia, particularly audits and assignments relating to cooperation partners that the Embassy of Sweden in Lusaka, on behalf of Sweden or Sida (The Swedish International Development Cooperation Agency), has an agreement with.

Only the Embassy of Sweden in Lusaka will be entitled to make call offs from the Framework Agreement and the Embassy of Sweden in Lusaka will be the contract holder

4.3 The Processor may process personal data only for the purpose of carrying out the obligations set out in the Main Agreement and only in accordance with the purposes described in Clause 4.2 of this Agreement.

Categories of Data Subjects

4.4 The personal data to be processed concern the following categories of data subjects: Employees and business partners.

Type of personal data processed

4.5 The personal data processed is of the following nature: Name, address, e-mail, phone number, date of birth.

Sensitive personal data processed (if applicable)

4.6 The processing relates to the following sensitive personal data:

Other protected personal data (if applicable)

4.7 The processing relates to the following privacy-sensitive personal data: Eventual personal information when there is suspicion of mismanagement, fraud or breach of agreement, such as but not exclusively debts, criminal records.

5 Controller's obligations

5.1 The Controller undertakes to ensure that there is a legal basis for the processing operations under Clause 4 and to draw up written instructions to enable the Processor and, where appropriate, Subprocessors, to perform their obligations under this Agreement.

5.2 The Controller is responsible for providing information under applicable legislation to the data subjects on the processing of personal data, consulting with the Swedish Authority for Privacy Protection where necessary, and otherwise ensuring that the processing of personal data by the Controller is lawful.

5.3 The Controller shall promptly provide information on any circumstances that may entail a need for changes in the way in which the Processor processes personal data and that may affect its obligations. The Controller shall also inform the Processor of any action by third party, including the Swedish Authority for Privacy Protection and the data subject, in relation to the processing.

6 Obligations of the Processor

Personal Data Processing

6.1 The Processor undertakes to process only contractual personal data in accordance with the Main Agreement and the Controller's instructions in this Agreement.

6.2 The Processor also undertakes to process the personal data in accordance with applicable data protection legislation and to keep up-to-date with and respect applicable laws that may have an impact on the processing of personal data under this Agreement.

6.3 The Processor and person(s) working under the Processor's supervision may only process personal data in accordance with *the purposes* and *instructions* set forth in this Agreement. The Controller reserves the right to update or clarify these instructions.

6.4 In the event that the Processor lacks instructions necessary for the performance of the Agreement, the Processor shall promptly, inform the Controller of his or her position and wait for such instructions which the Controller considers required. The Processor shall inform the Controller if the Processor becomes aware that personal data has been processed in violation of the Controller's instructions or the Personal Data Processing Agreement.

6.5 If data subjects, the Swedish Authority for Privacy Protection or other third parties request information from the Processor concerning the processing of personal data, the Processor shall refer them to the Controller. The Processor may not disclose personal data or other information concerning the processing of personal data without the prior written consent of the Controller, unless the disclosure obligation is provided in EU law or an applicable national law of a member state.

6.6 The Processor shall promptly inform the Controller of any contact from the Swedish Authority for Privacy Protection or other supervisory authority that is or may be relevant to the processing of personal data under this Agreement. The Processor shall not be entitled to represent the Controller or act on behalf of the Controller in relation to the Swedish Authority for Privacy Protection or other regulatory authorities.

6.7 The Processor shall assist the Controller in producing information requested by the Swedish Authority for Privacy Protection or the data subject, and will facilitate the Controller's performance of its obligations in relation to data subjects, such as the right to information, the right of rectification, the right of erasure or limitation of processing and the right to data portability.

Storage of documents, public access and disclosure of documents on request and confidentiality

6.8 The general documents handled by the Processor on behalf of the Controller constitute and remain part of the Controller's general documents pursuant to Chapter 2, Section 10, Law on the Freedom of the Press.

6.9 The Processor shall keep the Controller's data and documents logically separate from the data and documents of the Processor and other customers.

6.10 The Processor and the personnel working under this Personal Data Processing Agreement shall not orally, through the disclosure of documents or in any other way, disclose the information that he or she accesses in connection with this Agreement. The confidentiality obligation applies both during the term of the Agreement and after its termination.

6.11 The Processor shall ensure that all employees, consultants and other persons for whom the Processor is responsible and who process the personal data are bound by the confidentiality obligation. However, this is not required if they are already subject to a penalty sanctioned confidentiality obligation under law. The Processor also undertakes to ensure that there are confidentiality agreements with subprocessors, if any, and confidentiality agreements between the subprocessors and their personnel.

6.12 If data processed by the Processor on behalf of the Controller is requested, the Processor shall, as part of processing the request, consult an authorized representative of the Controller. The Processor and subprocessors, if any, may not disclose data or other information covered by this Agreement without the written instructions of the Controller.

Security of personal data processing

The Processor undertakes to take all appropriate technical and organisational security measures in accordance with the Data Protection Legislation or other relevant legislation and take any measures as set out in the instructions to protect personal data.

6.12 The Processor shall work systematically with information security. The Processor shall have procedures and tools to prevent unauthorized processing, destruction, alteration or unauthorized access to personal data.

6.13 When computer equipment and removable storage media of the Processor are not supervised, the equipment and media must be locked in order to be

protected against unauthorised use, interference and theft. Otherwise, the personal data shall be encrypted.

6.14 Where fixed or removable storage media containing personal data is no longer used for its purpose, the personal data shall be erased in such a way that they cannot be recreated.

6.15 Personal data transmitted via data communications controlled by the Processor shall be protected by encryption.

6.16 Access to sensitive and other types of privacy-sensitive personal data requires two-factor authentication.

6.17 The Controller has the right to investigate all types of security and personal data breaches.

Permissions

6.18 The Processor shall be responsible for having in place procedures for the allocation, alteration, deletion and regular review of its staff's permissions to access the Controller’s personal data. Permissions shall only be assigned to personnel who work with the assignment.

Logging

6.19 The Processor shall, upon request from the Controller, be able to provide logs of the personnel who have obtained access to personal data.

6.20 The Processor may use the information in the logs only as required to maintain the functionality and quality of IT systems and to control access to personal data.

Backup

6.21 The Processor shall ensure that the personal data are regularly transferred to backups, that the copies shall be kept separate and well protected so that the personal data can be recreated after a disruption and that there is a procedure for readback tests. The Processor shall comply with the backup procedures provided by the Controller.

Transfer to third countries

6.22 Personal data processed in connection with this agreement may only be transferred to another country if it is a country within the EU / EEA or a country that has a decision from the EU Commission on an adequate level of protection for personal data according to Art. 45 General Data Protection Regulation.

6.23 The Processor may not, without the written consent of the Controller, transfer any personal data to a country outside the EU/EEA area. This prohibition also applies to technical support, maintenance and similar services.

6.24 If the Controller has accepted the processing of personal data in a third country, the Processor is responsible for ensuring that the transfer to such third country takes place in accordance with the applicable data protection rules (e.g. Chapter V of the Data Protection Regulation).

Security incident

6.25 The Processor undertakes to assist the Controller in fulfilling its obligations in the event of a personal data breach. In case of suspected or confirmed security breach, the Processor shall immediately investigate the incident and take appropriate measures to remedy the incident and prevent a recurrence. The Processor shall also immediately inform the Controller of the incident or suspected incident and provide a description thereof.

6.26 The description shall include information necessary for the performance of the Controller's obligations according to Data Protection Legislation and shall give an account of:

1. the nature of the personal data breach and, where possible, the categories and number of affected data subjects,
2. the likely consequences of the personal data breach, and
3. measures taken or proposed, and measures to mitigate the potential negative effects of the personal data breach.

Unless all the necessary information can be provided directly, information may be provided gradually, but promptly.

Impact Assessment and Prior Consultation

6.27 The Processor shall, at the request of the Controller, assist the Controller in impact assessments and prior consultation.

7 Subprocessors

7.1 The Processor may, upon the Controller's consent, assign the processing of the Controller's personal data to one or more subprocessors. In each such situation, the Processor shall conclude an individual Personal Data Processing Agreement with each subprocessor. The agreement shall clearly state that the conditions applicable to the processing of personal data by the Processor under this Agreement shall also apply to the processing assigned to the subprocessor. The Controller shall be informed already at the planning stage, if applicable, of subprocessors that need to be hired and shall be given the opportunity to object to selected subprocessors within a reasonable time.

7.2 The Processor shall ensure, in agreements with subprocessors or where special instructions are given to a subprocessor, that the subprocessor handles the Controller's personal data in accordance with this Agreement. The Processor shall be particularly attentive to the fact that information management in the public sector may also be subject to other specific regulations regarding public access, confidentiality or archiving, which must be observed.

7.3 A subprocessor may assign the processing to another processor only if it is carried out on the same conditions applicable to the Processor's assignment of the processing.

7.4 The Processor shall, at the Controller's request, provide a copy of those parts of the Personal Data Processing Agreement concluded with the subprocessor and any other information necessary to show that the Processor has fulfilled its obligations under this Personal Data Processing Agreement.

7.5 The Processor shall keep a list, which shall be correct and up-to-date at each time, showing the subprocessors hired to process personal data under this Agreement and make such list available to the Controller. The list shall indicate in particular the countries in which the subprocessor processes the personal data and the types of processing operations carried out by the subprocessors.

7.6 If a subprocessor fails to perform its data protection obligations, the Processor shall be fully liable in relation to the Controller.

7.7 If this Agreement is terminated, the Processor and subprocessors may not continue to process personal data subject to the Agreement. In such cases, the personal data shall be returned or erased in accordance with the Parties' agreement and Clause 11 of this Agreement.

8 Operation and Maintenance

8.1 General contract terms and conditions of operation and maintenance are set out in the Main Agreement. Clauses 8.2 and 8.3 become applicable in cases where they form part of the nature of the agreement according to the Main Agreement.

8.2 When repair and servicing of computer equipment, used to store the Controller's personal data, is performed by a person other than the Processor, an agreement governing security and confidentiality shall be made with the service provider.

8.3 During service visits, service must be carried out under the supervision of the Processor. If this is not possible, storage media containing personal data must be removed.

8.4 Service via remote computer communication is only permitted via Sida's approved remotely controlled solutions. Service personnel shall be granted access to the system only when service is carried out.

9 Auditing and Visits

9.1 The Controller may, itself or through third parties, at its own expense, carry out audits of the Processor and its subprocessors or otherwise verify that the Processor's processing of personal data complies with the Personal Data Processing Agreement. In the event of such audits or verifications, the Processor shall provide the Controller's representatives with necessary assistance to conduct the audit.

9.2 The Controller's representatives shall be entitled to inspect the hardware and software used for the processing of personal data covered by this Agreement and access to the physical premises where equipment and other hardware and software is located.

9.3 The Processor shall allow the regulatory authority access to conduct on-site inspections.

10 Liability for damages

10.1 Liability for damages is regulated in accordance with Article 82 of the Data Protection Regulation. The Controller is entitled to a refund by the Processor of any fine imposed on the Controller due to breach of any provision of this Agreement or applicable data protection provision where such breach was caused by the Processor or by a party for whom the supplier is responsible. Where both the Controller and the Processor have participated in the breach, the Processor shall only compensate the Controller for the part of the fine corresponding to the Processor's share of liability.

11 Termination of personal data processing

11.1 In connection with termination of this Agreement, the Processor and, where applicable, any subprocessors shall permanently remove personal data from storage media used so that the data can no longer be recreated. This measure shall be fully completed no later than 180 days after termination of the Agreement.

If the Controller so requires, the Processor shall, prior to such deletion, return all transferred personal data to the Controller. Unless otherwise agreed or manifestly obvious based on circumstances, the personal data shall be transferred in a format that is readable or possible to use in other contexts. This means that not only the personal data shall be provided, but also any other logical information necessary to use the personal data. Furthermore, log files, audit data, access data and similar metadata must also be provided. Such data must also be provided in a format that the Controller can use.

12 Term, amendment and termination

12.1 This Personal Data Processing Agreement is valid as long as the Processor processes personal data on behalf of the Controller under the Main Agreement or until a new Personal Data Processing Agreement takes effect.

12.2 The Processor has no independent right to amend this Agreement.

13 Disputes and applicable law

13.1 Disputes regarding the interpretation or application of this Agreement shall be settled in accordance with the dispute resolution clause in the Main Agreement.

14 Signatures

The Personal Data Processing Agreement has been executed as two identically worded copies of which each Party has taken its own.

Authorised signatory of the Controller	Authorised signatory of the Processor
[insert place and date].	[insert place and date].
Signature	Signature
Name in block letters [insert title], Sida	Name in block letters [title and party]