Data Processing Agreement (ARVODI 2025)

Contract number: [...].

The undersigned:

1. The State of the Netherlands, which has its seat in The Hague,
represented by the Minister of Economic Affairs and Climate Netherlands Enterprise Agency (RVO),
legally represented in this matter by drs. J.L.M. Judith Arends, Head of CBI, Director International Programs,
hereinafter referred to as 'the Contracting Authority',

and

2. [Contractor's full name and legal form],
which has its registered office in [...],
legally represented in this matter by
[signatory's name],
hereafter referred to as 'the Contractor',

WHEREAS:

- In so far as the Contractor processes Personal Data for the Contracting Authority in the context of the Contract, the Contracting Authority qualifies as a Controller for the Processing of Personal Data and the Contractor as a Processor;
- The Parties to this Data Processing Agreement, as referred to in Article 28, paragraph 3 of the Regulation, wish to record their agreements on the Processing of Personal Data by the Contractor.

AGREE AS FOLLOWS:

Article 1. Definitions

Certain terms in this Data Processing Agreement are written with initial capitals. These terms are defined in the ARVODI 2025 or the Regulation, on the understanding that the definitions of a number of terms are geared to the Data Processing Agreement. In addition thereto, the following terms are thus defined below for the purposes of this Data Processing Agreement, regardless of whether they are used in the singular or plural or as verbs or nouns:

1.1 ARVODI 2025: the General Government Terms and Conditions for Public Service Contracts 2025.
1.2 Data Subject: the person whom the Personal Data concerns.
1.3 EEA: the European Economic Area, comprising all EU countries in addition to Liechtenstein, Norway and Iceland.
1.4 Personal Data Breach: a breach in security that leads to the accidental or unlawful destruction, loss, change or unauthorised disclosure of, or unauthorised access to, data that has been transferred, stored or Processed in any other way.
1.5 Recipient: a natural or legal person, public authority, agency or another body, to which the Personal Data is disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or member state law are not regarded as Recipients; the Processing of that data by those public authorities takes place in compliance with the data protection rules applicable to the purposes of the processing.

1.6 Contract: the agreement between the Contracting Authority and the Contractor [title] dated [date], reference number [number].
1.7 Personal Data: any data concerning an identified or identifiable natural person that is Processed by the Contractor for the Contracting Authority in the context of the Contr
1.8 Supervisory Authority: an independent public authority which is established by a member state pursuant to Article 51 of the Regulation.
1.9 Regulation: 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 (General Data Protection Regulation).
1.10 Processor: a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
1.11 Data Processing Agreement: this agreement including its recitals and the accompanying schedules.
1.12 Processing: any operation or any set of operations concerning Personal Data or any set of Personal Data, carried out in the context of the Contract via automated or manual procedures, including in any case the collection, recording, organisation, structuring, storage, updating or modification, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.
1.13 Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or member state law, the Controller or the specific criteria for its nomination may be provided for by Union or member state law.

Article 2. Object of this Data Processing Agreement

2.1 This Data Processing Agreement governs Processing by the Contractor in the context of the Contract and is inextricably linked to the Contract.
2.2 The nature and purpose of the Processing, the type of Personal Data and the categories of Personal Data, Data Subjects and Recipients are set out in Schedule 1.
2.3 The Contractor guarantees that the appropriate technical and organisational measures will be taken in order to ensure that Processing complies with the requirements of the Regulation and that the rights of the Data Subject are protected.
2.4 The Contractor guarantees compliance with the requirements of the applicable legislation relating to the Processing.

Article 3. Entry into force and term

3.1 This Data Processing Agreement enters into force as soon as it has been signed by the Parties.
3.2 This Data Processing Agreement terminates after the Contractor has erased or returned all Personal Data and has deleted existing copies in accordance with article 10 of this Data Processing Agreement.
3.3 Early termination of this Data Processing Agreement is not possible.

Article 4. Scope of the Contractor's Processing competence

4.1 The Contractor will Process Personal Data only for, and on the basis of written instructions from, the Contracting Authority, unless the Contractor is required by a statutory regulation to carry out Processing. In that case the Contractor will notify the Contracting Authority of such a statutory regulation prior to the Processing, unless that statutory regulation prohibits such notification on important grounds of public interest.
4.2 The Contractor has no control over the purpose or means of the Processing within the meaning of the Regulation.

Article 5. Security of the Processing

5.1 Without prejudice to article 2.3 of this Data Processing Agreement, the Contractor will implement the technical and organisational security measures described in Schedule 2.

5.2 The Parties recognise that guaranteeing an appropriate level of security may require additional security measures to be implemented on an ongoing basis. The Contractor guarantees a level of security appropriate to the risk.
5.3 At the express written request of the Contracting Authority, the Contractor will adopt additional measures to ensure the security of the Personal Data.
5.4 The Contractor will not Process any Personal Data outside the EEA unless it has obtained express written consent from the Contracting Authority to do so, subject to further conditions if necessary, and barring statutory obligations to the contrary.
5.5 The Contractor will inform the Contracting Authority without unreasonable delay as soon as it becomes aware of any unlawful Processing of Personal Data or failure in (or failure to comply with) the technical and organisational security measures referred to paragraphs 1 and 2.
5.6 The Contractor will assist the Contracting Authority in ensuring compliance with the obligations under Articles 32 to 36 inclusive of the Regulation.

Article 6. Duty of Confidentiality of the Contractor's Staff

6.1 The Personal Data is confidential as referred to in article 11.1 of the ARVODI 2025.
6.2 The Contractor guarantees that, as referred to in article 11.2 of the ARVODI 2025, its Staff have undertaken to observe the duty of confidentiality.

Article 7. Subprocessor

If the Contractor, with due regard for the provisions of article 6 of the ARVODI 2025, engages another Processor to carry out processing activities for the Contracting Authority, the other Processor must be bound by an agreement imposing the same data protection obligations as those imposed by this Data Processing Agreement.

Article 8. Assistance concerning rights of Data Subjects

8.1 Taking into account the nature of the Processing, the Contractor will assist the Contracting Authority by means of appropriate technical and organisational measures, in so far as this is possible, in the fulfilment of the Contracting Authority's obligation to respond to requests for exercising the Data Subject's rights laid down in chapter III of the Regulation.
8.2 Each of the Parties will bear any costs they incur in connection with paragraph 1.
8.3 The Contractor will send a request from a Data Subject to the Contracting Authority as soon as possible.

Article 9. Personal Data Breach

9.1 The Contractor will inform the Contracting Authority, without unreasonable delay, as soon as it becomes aware of any Personal Data Breach, in accordance with the agreements set out in Schedule 3.
9.2 After reporting an incident as described in paragraph 1, the Contractor will also inform the Contracting Authority of developments relating to the Personal Data Breach.
9.3 Each of the Parties will bear any costs they incur in relation to the Personal Data Breach.

Article 10. Return or erasure of Personal Data

10.1 Once the Contract expires or earlier as agreed the Contractor will ensure that it erases all the Personal Data or returns it to the Contracting Authority, whichever the Contracting Authority prefers, and deletes existing copies, unless statutory regulations require the storage of the Personal Data.
10.2 The Parties may agree retention periods for separate Personal Data or categories of Personal Data. Once the agreed retention period has expired, the Contractor will ensure the erasure or return and the deletion of copies of the Personal Data concerned unless statutory regulations require the storage of the Personal Data.
10.3 The Contractor will erase or return the Personal Data within 4 weeks following the expiry of the Contract or earlier as agreed, failing which the Contractor will owe a penalty of € 500.- per day, up to a maximum of the value of all awarded further contracts within the

framework agreement. Payment of the penalty does not affect the Contractor's obligations under article 10 or its liability for compensating any damage caused by the breach.

10.4 The Personal Data will be returned in the form and manner stipulated by the Contracting Authority.

Article 11. Obligation to supply information and audit obligation

11.1 The Contractor will provide all necessary information to show that the obligations set out in this Data Processing Agreement have been and are being fulfilled.

11.2 The Contracting Authority can perform an audit (or have an audit performed) of the Processing activities that fall under the Data Processing Agreement if concrete circumstances give reason to do so. The Contractor will cooperate fully with audits, including audits among the Contractor's Staff, unless it cannot reasonably be expected to do so.

11.3 The Contractor will immediately notify the Contracting Authority if, in its opinion, an instruction from the Contracting Authority in the context of article 11, paragraph 1 and/or paragraph 2 of this Data Processing Agreement breaches a statutory regulation relating to data protection.

11.4 The Parties themselves will bear the costs they incur in connection with the information provision and audits referred to in this article, including the costs of third parties engaged by them.

11.5 The Contracting Authority is authorised at all times to propose further measures prompted by the information obtained under this article. The Contractor is obliged to carry out these measures in so far as is reasonable.

The Hague, [date]

the Minister of Economic Affairs on behalf of
and commissioned by Mr J. Arends,
Head of CBI

[signatory]

[signatory's name]

[place], [date]

[Contractor's name]

[signatory]

[signatory's name]

Intern gebruik

Schedule 1. Processing Personal Data

This schedule must in any case specify:

Overview of Processing

The subject-matter, nature and purpose of the Processing	Collection of information regarding social compliance initiatives of coffee exporters in Colombia (2-20 companies). Data includes export performance, number of employees, key results achieved in participation. This data will be used to evaluate and enhance the CBI project. The processing tool used is SAGE/HBAT (CBI internal CRM system)
The type of Personal Data	Regular personal date (name, contact details, address) Company details (name, details) Company performance data (turnover per year, number of employees, completed programme activities)
The categories of Personal Data	Regular personal date Company performance data
The categories of Data Subjects	Coffee exporters (SMEs and cooperatives) in Colombia
The categories of Personal Data Recipients	CBI programme manager, CBI MEL advisors, and hired experts (contractor) who has access to the project data in SAGE/HBAT
Location of Personal Data Processing	The regular personal data collected and processed within Microsoft Excel are processed outside EEA

< if applicable>
Subprocessor(s)

Subprocessor's name and contact details	
Subprocessor's commercial register number	
The subject-matter, nature and purpose of the Processing	
The type of Personal Data	
The categories of Personal Data	
The categories of Data Subjects	
The categories of Personal Data Recipients	
Location of Personal Data Processing	
……..	

Schedule 2. Appropriate technical and organisational measures

Within the national government, the Government Information Security Baseline (BIO) serves as the basis for the organization of information security.
The Contractor takes appropriate technical and organisational measures based on the risk of the Processing (see article 1.12 for a definition of processing) The following is seen as a minimum and obligatory:

Information security measures
Applicable to all processing of **regular person data**

1. **Access control**
   - Access to systems is permitted only for authorized users.
   - Accounts are personal and not shared.
   - Strong passwords are used (minimum 12 characters).
   - Accounts of departed employees are deactivated within 24 hours.
2. **Stronger access security**
   - Multi-factor authentication (MFA) for:
   - All accounts
   - external access
   - Periodic review of access rights (at least annually).
3. **Governance and organization**
   - The processor has a designated person responsible for information security (e.g., security officer or IT manager).
   - Basic documentation regarding security measures and procedures is available.
   - Security measures are periodically evaluated and adjusted if necessary.
4. **Devices and systems**
   - Devices and servers are provided with regular security updates.
   - Antivirus/endpoint protection is active on workstations. Unused accounts and services are deleted or disabled.
5. **Data protection**
   - Excel files with personal information may not be sent by regular email. The RVO application 'SecureTransfer' must be used. Ask the CBI project manager for instructions.
   - Data is used only for the contractually agreed purpose.
   - Unnecessary copies of data are prevented.
   - Data is deleted or returned at the end of the contract.
6. **Incident management**
   - Security incidents are recorded and investigated.
   - Incidents impacting customer data are reported to the Netherlands Enterprise Agency without undue delay.
7. **Personnel**
   - Employees are bound by a confidentiality obligation.
   - Employees receive basic awareness training on information security.

Add here your certifications and other qualifications in relation to data protection

Certificates	**Organizational unit/service to which the certificate relates**	**Certificate validity period**	**Statement of Applicability**

Other qualifications and/or data security measures:

Schedule 3. Agreements on Personal Data Breaches

The agreements on how the Contractor will inform the Contracting Authority of Personal Data Breaches is specified in this schedule.

Background
The data breach reporting obligation has been in force since 1 January 2016. This reporting obligation requires organizations (both businesses and government agencies) to report any serious data breach to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) without delay. Under specific circumstances, they are obliged to report the data breach to the Data Subjects (the individuals whose Personal Data are involved in the breach) as well.
As the Contractor will be processing Personal Data within the framework of performing the agreement, the Contractor is obliged to report a breach involving personal data to the Contracting Authority as soon as it is discovered, without unreasonable delay (Article 33(2) of the GDPR).

Cooperation
The Data Breach Response Team (DRT) coordinates the handling of the data breach for the Ministry of Economic Affairs and Climate Policy as well as the reporting thereof to the Dutch Data Protection Authority and – where necessary – the Data Subjects. The Contractor must cooperate fully by providing the DRT with all the requested information.

Minimum information that the contractor must supply:

Details of its organisation
Details of the person reporting the breach
Date and time of discovery of suspected Personal Data Breach
Nature of the Personal Data Breach
Type, categories and quantity of Personal Data and Data Subjects
Probable consequences of the Personal Data Breach
Measures proposed or taken by the Contractor to tackle the Personal Data Breach including, where relevant, measures to limit its possible negative consequences.

Even if not all of the above information is available yet, the Contracting Authority's contact person for data breaches must be contacted without delay.

Examples of data breaches:
- loss or theft of a laptop, smartphone, flash drive, and so on, also if it concerns encrypted data;
- accidental publication of Personal Data.
- sending an email with names in the CC rather than in the BCC if the addressees have nothing to do with each other, or sending an email to the wrong address;
- being the victim of a phishing email or hack;
- illegal transfer of usernames/login codes or having access to files which you are not (or no longer) authorised to access;
- destruction of a data base containing Personal Data as a result of human error, without the presence of a back-up.

To be completed by the Contractor:
Contact details for data breaches:
E:
T:
Availability:

To be completed by the Contracting Authority:
Contact details for data breaches
E: rvoinformatiebeveiliging@rvo.nl
Availability: Monday to Friday from 07:30 to 18:30 CET