Data Processing Agreement (ARVODI 2025)

Expertise for the CBI project Bangladesh Circular Apparel & Textile
Contract number: [...].

The undersigned:

1. The State of the Netherlands, which has its seat in The Hague,
represented by the Minister of Economic Affairs, Netherlands Enterprise Agency (RVO),
legally represented in this matter by
drs. J.L.M. Arends,
Head of CBI,
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',

jointly referred to as 'the Parties';

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 Contract.

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, the Contractor will erase the Personal Data or return it to the Contracting Authority, whichever the Contracting Authority prefers. The Contractor will delete any copies, barring statutory rules to the contrary.

10.2 The Contractor will erase the Personal Data within 4 weeks following the expiry of the Contract, failing which it will be fined € 500,- per day, up to a maximum of € [*estimated value of Contract/estimated value of all Further Agreements*].

10.3 The Personal Data will be returned to the Contracting Authority in the format 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.

Done on the later of the two dates stated below and signed in duplicate.

The Hague, [date]	City/place, [date]
FOR THE MINISTER OF ECONOMIC AFFAIRS	FOR [CONTRACTOR],
on behalf of and commissioned by	
drs. J.L.M. Arends,	
Head of CBI,	
of the Netherlands Enterprise Agency (RVO),	
Esther Zandt	signatory's name
Team Manager Procurement Office	signatory's position

Schedule 1. Processing Personal Data

This schedule must in any case specify:

Overview of Processing

To be completed by the Contracting Authority (the Controller)	
Name of Controller including contact details	The Minister of Economic Affairs, on behalf of the general director of the Netherlands Enterprise Agency (RVO): Mr. A. Choho (General director of RVO) PO Box 93144, 2509 AC The Hague
Contact details of the Controller's representative	Sustainable Economic Development Directorate, CBI drs. J.L.M. Arends (Head of CBI) PO Box 93144, 2509 AC The Hague
Contact details DPO of the Controller	Data Protection Officer of the Ministry of Economic Affairs Bureau Bestuursraad PO Box 20401 2500 EK The Hague PbFG@minezk.nl
The subject/nature and purpose of the Processing	The data processing activities for the execution of the CBI project 'Bangladesh circular apparel & textiles' and include: • **Data collection from exporting companies:** Collection of information regarding environmental compliance, natural dyeing and/or recycled yarn initiatives of apparel and textile SMEs in Bangladesh (approximately 5-10 companies). The data includes export performance, number of employees, and key results achieved from participation in the CBI project. This data will be utilized to evaluate and enhance the impact of the CBI project on the Bangladesh circular apparel & textiles sector in Bangladesh. The processing tool used is Sage/HBAT (CBI internal CRM system) and audit forms in Excel. • **Online trainings and coaching sessions:** Experts that organize (online) trainings and coaching sessions will register attendance and collect feedback or evaluations. The processing tool used is Excel.
The type of Personal Data	**Regular personal data:** • Name (first name, last name, prefix, initials) • Contact details (e-mail address) **Company performance data:** • Turnover per year • Number of employees. • Completed program activities • Other key performance metrics.

	Other partner data: • Organization name and contact details • Organizational performance data.
Description of categories of Personal Data	• **Regular personal data:** This includes basic identity and contact information of individuals involved in the project. • **Company performance data:** This encompasses various quantitative metrics that reflect the company's performance.
Description of categories Data subjects	• Apparel & Textile SMEs in Bangladesh. • Key sector stakeholders in the Bangladeshi Apparel and Textile sector, including associations and women networks.
Description of categories of recipients of Personal Data	CBI Programme Managers, CBI MEL advisors and hired experts (contractor) who have access to the data of this project in Sage/HBAT.
Location Processing Personal Data	Within the EEA / (partly)outside the EEA

To be completed by the Contractor (the processor)	
Name Processor including contact details	
Contact details of Processor representative	
Contact details DPO of the Processor	
Will the data be transferred to one or more countries outside the EEA?	Yes/No

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's security must meet at least the same requirements as the BIO prescribes for the following components: BBN-2
- The Contractor implements additional measures based on the risk of the Processing, which have been determined, for example, as a result of a Privacy Impact Assessment (PIA). An overview of these measures is included below.

Certificates	Organizational unit/service to which the certificate relates	Certificate validity period	Statement of Applicability
Not Applicable			

Additional security Requirements:

For the collection of personal data, the following security requirements must be observed by (local) experts:

Control number	Control description
8. Asset management	
8.1	Responsibility for company assets
8.1.1	Asset Inventory: Information, other assets associated with information, and information processing facilities should be identified, and an inventory of these assets should be established and maintained.
8.1.2	Ownership of Assets: Assets maintained in the inventory statement should have an owner.
8.1.3	Acceptable use of assets: Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented and implemented.
8.1.4	Return of Assets: All employees and external users must return all organizational assets in their possession upon termination of their employment, contract or agreement.
8.2	Information classification
8.2.1	Classification of information: Information should be classified with respect to legal requirements, value, importance and susceptibility to unauthorized disclosure or modification.
8.2.2	Information labeling: To label information, an appropriate set of procedures should be developed and implemented in accordance with the information classification scheme established by the organization.
8.2.3	Asset Handling: Asset handling procedures should be developed and implemented in accordance with the information classification scheme established by the organization.
8.3	Handling media
8.3.1	Removable media management: Procedures for managing removable media should be implemented in accordance with the classification scheme established by the organization.
8.3.2	Disposal of media: Media should be disposed of in a safe and secure manner when it is no longer required, in accordance with formal procedures.
8.3.3	Physically transferring media: Media containing information should be protected from unauthorized access, misuse, or corruption during transit.
9. Access security	
9.1	**Business requirements for access security**
9.1.1	Access security policy: An access security policy should be established, documented and assessed based on business and information security requirements.
9.1.2	Access to networks and network services: Users should only access the network and network services for which they are specifically authorized.
9.2	**Management of user access rights**
9.2.1	Registration and Logout of Users: A formal registration and logout procedure should be implemented to allow assignment of access rights.
9.2.2	Granting User Access: A formal user access granting procedure should be implemented to grant or revoke access rights for all types of users and for all systems and services.

9.2.3	Managing special access rights: The assignment and use of special access rights should be limited and controlled.
9.2.4	Management of user secret authentication information: The assignment of secret authentication information should be managed through a formal management process.
9.2.5	Review of user access rights: Asset owners should regularly review user access rights.
9.2.6	Revoking or modifying access rights: All employees' and external users' access rights to information and information processing facilities should be deleted upon termination of their employment, contract or agreement, and modified if changes occur.
9.3	**User Responsibilities**
9.3.1	Using Secret Authentication Information: Users should be required to adhere to organizational practices when using secret authentication information.
9.4	Access protection of system and application
9.4.1	Restricting access to information: Access to information and system functions of applications should be restricted in accordance with the access control policy.
9.4.2	Secure login procedures: Where required by access security policies, access to systems and applications should be controlled by a secure login procedure.
9.4.3	Password management system: Password management systems should be interactive and ensure strong passwords.
9.4.4	Using special system tools: The use of system tools that have the ability to circumvent system and application controls should be limited and closely controlled.
9.4.5	Access protection on program source code: Access to the program source code should be restricted.
11. Physical and environmental security	
11.1	Secure areas
11.1.1	Physical Security Zone: Security zones should be defined and used to protect areas containing sensitive or essential information and information processing facilities.
11.1.2	Physical access security: Secured areas should be protected by appropriate access security to ensure that only authorized personnel are allowed access.
11.1.3	Securing offices, spaces and facilities: Physical security should be designed and applied to offices, spaces and facilities.
11.1.4	Protect against external threats: Physical protection should be designed and applied against natural disasters, malicious attacks or accidents.
11.1.5	Working in secure areas: Procedures should be developed and applied for working in secure areas.
11.1.6	Loading and unloading location: Access points such as loading and unloading locations and other points where unauthorized persons can enter the site should be controlled and, if possible, shielded from information processing facilities to prevent unauthorized access.
11.2	**Equipment**
11.2.1	Location and protection of equipment: Equipment should be located and protected in such a way that risks from external threats and hazards, as well as the possibility of unauthorized access, are reduced.
11.2.2	Utilities: Equipment should be protected against power outages and other disruptions caused by utility disruptions.
11.2.3	Cabling security: Power and telecommunications cables that transmit data or support information services should be protected against interception, disruption or damage.
11.2.4	Equipment maintenance: Equipment should be properly maintained to ensure its continued availability and integrity.
11.2.5	Asset Removal: Equipment, information and software should not be removed from site without prior approval.
11.2.6	Security of equipment and assets off-site: Assets located off-site should be secured, taking into account the various risks of working off-site.
11.2.7	Secure disposal or reuse of equipment: All parts of the equipment that contain storage media should be verified to ensure that sensitive data and licensed software have been removed or reliably securely overwritten prior to disposal or reuse.
11.2.8	Unmanaged user equipment: Users should ensure that unmanaged equipment is adequately protected.
11.2.9	Clear desk and clear screen policies: A clear desk policy for paper documents and removable storage media and a clear screen policy for information processing facilities should be established.
12. Business operations security	
12.1	Operating procedures and responsibilities

12.1.1	Documented operating procedures: Operating procedures should be documented and made available to all users who need them.
12.1.2	Change management: Changes in the organization, business processes, information processing facilities and systems that affect information security should be controlled.
12.1.3	Capacity management: Resource usage should be monitored and aligned, and expectations should be set for future capacity requirements to ensure required system performance.
12.1.4	Separation of development, test and production environments: Development, test and production environments should be separated to reduce the risk of unauthorized access to or changes to the production environment.
12.2	**Protection against malware**
12.2.1	Malware controls: To protect against malware, detection, prevention and remediation controls should be implemented, along with appropriate user awareness.
12.3	**Backup**
12.3.1	Backup of information: Backup copies of information, software and system images should be created and tested on a regular basis in accordance with an agreed upon backup policy.
12.4	**Reporting and monitoring**
12.4.1	Event Logging: Event logs that record user activities, exceptions, and information security events should be created, retained, and reviewed regularly.
12.4.2	Protecting information in log files: Log facilities and information in log files should be protected against falsification and unauthorized access.
12.4.3	Administrator and Operator Logs: Activities of system administrators and operators should be recorded and the logs should be protected and reviewed regularly.
12.4.4	Clock synchronization: The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source.
12.5	**Mastery of operational software**
12.5.1	Installing software on operational systems: Procedures should be implemented to control the installation of software on operational systems.
12.6	**Technical vulnerability management**
12.6.1	Technical Vulnerability Management: Information on technical vulnerabilities of information systems in use should be obtained in a timely manner, the organization's exposure to such vulnerabilities should be assessed, and appropriate measures should be taken to address the associated risk.
12.6.2	Software Installation Restrictions: Rules for user installation of software should be established and implemented.

The above measures are a selection of measures from the BIG (level BBN-2)/ISO27001 that are applicable to self-employed entrepreneurs.

- Excel files with personal information may not be sent by regular email. The RVO application 'SecureTransfer' must be used. The CBI project manager will provide a link to upload the files safely..

After the expert/business export coach has received the Excel file, it is placed in Sage/HBAT. The expert/business export coach has an account in Sage/HBAT.

Schedule 3. Agreements on Personal Data Breaches

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.

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: Monday - Friday

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