Rijksdienst voor Ondernemend Nederland

Data processing agreement

International Development, EnDev / Third party

Contract number: 202403001

The undersigned:

1. The State of the Netherlands, which has its seat in The Hague,
represented by the Minister for Foreign Trade and Development,
legally represented in this matter by drs. J.L.M. Arends,
Head of International Development,
Directorate International Programs,
hereafter referred to as 'the Contracting Authority',

and

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

jointly referred to as 'the Parties';

WHEREAS:

- Insofar as the Contractor processes Personal Data for the Contracting Authority in the context of the Contract, the Contracting Authority, under article 4 (7) and (8) of the Regulation, 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 article 1 of the General Government Terms and Conditions for Public Service Contracts 2018 (ARVODI 2018). In derogation therefrom or in addition thereto, the following terms are defined below for the purposes of this Data Processing Agreement:

1.1 Data Subject: the person whom the Personal Data concerns.

1.2 Personal Data Breach: a breach in security that leads to the accidental or unlawful destruction, loss, change or unauthorised provision of, or unauthorised access to, data that has been transferred, stored or processed in any other way.

1.3 Contract: the Contract (EnDev Energy Enterprise Coach) between the Contracting Authority and the Contractor.
[name] dated [date], reference number 202303001.

1.4 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.

1.5 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).

1.6 Data Processing Agreement: this agreement including its recitals and the accompanying schedules.

1.7 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.

Article 2 Object of this Data Processing Agreement

2.1 This Data Processing Agreement governs the Processing of Personal Data by the Contractor in the context of 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(s) are protected.

2.4 The Contractor guarantees compliance with the requirements of the applicable legislation relating to the Processing of Personal Data.

Article 3 Entry into force and duration

3.1 This Data Processing Agreement enters into force as soon as it has been signed by both Parties.

3.2 This Data Processing Agreement terminates after and insofar as the Contractor has deleted or returned all Personal Data in accordance with article 10.

3.3 Neither of the Parties may terminate this Data Processing Agreement before the Contract terminates.

Article 4 Scope of Contractor's Processing competence

4.1 The Contractor will Process the Personal Data exclusively for and on the basis of written instructions from the Contracting Authority barring statutory rules to the contrary that apply to the Contractor.

4.2 If any instruction as referred to in paragraph 1 is deemed by the Contractor to contravene a statutory rule on data protection, the Contractor will notify the Contracting Authority of this prior to Processing, unless a statutory rule prohibits such notification.

4.3 If the Contractor is obliged to disclose Personal Data on the basis of a statutory rule, it will inform the Contracting Authority immediately, if possible prior to the disclosure.

4.4 The Contractor will have no control over the purpose or means of the Personal Data Processing.

Article 5 Security measures

5.1 In addition to article 15 of the ARVODI 2018, and 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 an appropriate level of security having regard to the risks entailed.

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 a European Union member state, unless it has obtained express written approval to do so from the Contracting Authority and barring statutory obligations to the contrary.

5.5 If the Contractor discovers any illegal or unauthorised Processing or infringements of the security measures referred to paragraphs 1 and 2, it will inform the Contacting Authority without unreasonable delay.

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 13.1 of the ARVODI 2018.

6.2 At the request of the Contracting Authority, the Contractor will show that its Staff have undertaken to observe the duty of confidentiality referred to in article 13.2 of the ARVODI 2018.

Article 7 Subprocessor

If the Contractor, with due regard for the provisions of article 8 of the ARVODI 2018, 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

The Contractor will assist the Contracting Authority in fulfilling its obligation to respond to requests from Data Subjects to exercise the rights set out in chapter III of the Regulation.

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 the first paragraph, 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 connection with reporting incidents to the competent supervisory authority and the Data Subject.

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 €1,500,000.

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 will be fulfilled.

11.2 The Contractor will provide all necessary cooperation with respect to audits.

11.3 The Contracting Authority will have an independent party carry out an audit once every one and a half year.

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

The Hague, [date]
FOR THE MINISTER FOR FOREIGN TRADE AND DEVELOPMENT,
on behalf of and commissioned
by drs. J.L.M. Arends,
Head of International Development,
of the Netherlands Enterprise Agency (RVO),

J. van Putten
Team manager Procurement Office

The Hague, [date]

City/place, date 2024
[CONTRACTOR],

signatory's name
signatory's position

[place], [date]

Schedule 1 Processing Personal Data

This Schedule must in any case specify:

To be completed by the Contracting Authority (The Controller)	
Name of Controller including contact details	The Minister of Economic Affairs and Climate, 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	Directorate International Programs, drs. J.L.M Arends (Head of International Development) PO Box 93144, 2509 AC The Hague
Contact details DPO of the Controller	Privacy Control Team Netherlands Enterprise Agency avg@rvo.nl
The subject/nature and purpose of the Processing	The EnDev Energy Enterprise Coach gathers personal data in the form of names and contact details. This is necessary to collect (sensitive) company data about the companies that receive the support offered by this Assignment. Furthermore, the sex of the actors will be collected as part of the assignment includes reporting on this variable. The companies are SMEs focused on renewable energy access. This data includes turnover, number of employees, sales numbers, etc. This data gathering is needed for proper execution of the assignment as the business development support to these companies have to be adapted to the state of the companies. Furthermore, the impact of the business development support provided under this Assignment has to be monitored by comparing company data pre and post support. This data will be provided by the companies themselves, and will not become publicly available by the Contractor. This data will be shared via and stored on a to a proposed platform that is approved by the Contracting Authority, for example EZ&K NetFTP.
The type of Personal Data	**Regular personal data:** • Name (first name, last name, prefix, initials) • Contact details (e-mail address, phone number) • Sex • Position in organization
Description of categories of Personal Data	Regular personal data
Description of categories Data subjects	1. Energy Access SMEs within the geographical scope.

	2. EnDev partners (implementers, governmental organisations, financial institutions, NGO's, other BDS suppliers).
Description of categories of recipients of Personal Data	1. EnDev Energy Enterprise Coach 2. RVO 3. GIZ
Location Processing Personal Data	Within 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?	No

Sub-processor (s)

Name and contact details of sub-processor	
Trade register number of sub-processor	
The subject/nature and purpose of the Processing	
The type of Personal Data	
Description of categories of Personal Data	
Description of categories Data subjects	
Description of categories Recipients of Personal Data	
Location Processing Personal Data	

The information in the controller's records, obligatory under article 30 of the Regulation, can be used to complete this schedule.

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

Other qualifications:

To be completed Client:

Additional security Requirements:

The requirements, as stated in the Cloud Policy of the Ministry of Economic Affairs an Climate, apply:

1. The supplier has a valid ISO-27001 certification and the entire lifecycle of the cloud application falls within the scope of this certification.
2. There are agreements on how data and/or software will be transferred in the event of termination of the agreement and what obligations the supplier has in this regard (exit strategy).
3. The supplier undertakes to report security incidents relevant to the services provided to RVO directly to the RVO Security Office (rvoinformatieveiligheid@rvo.nl) within 4 hours of discovery, stating the client within RVO.
4. The supplier undertakes to resolve any security issues identified with regard to the public cloud application they supply. To this end, the supplier reports to RVO within 48 hours the period within which the solution has been realized.
5. The supplier undertakes to cooperate with audits in the field of information security and privacy initiated by the client.
6. The supplier undertakes to provide insight into which other parties are involved in the implementation of the agreement. Changes in the parties involved are communicated in writing to the client within RVO and to the 'RVO IMP Service Desk'.
7. There are agreements in place how the supplier passes on data to third parties within the contractual purpose of the client (e.g. backups, log files, telemetry, etc.). Explicit permission from the client is required for the transfer of data within the contractual purpose limitation to processors outside the EU/EEA area.
   There are agreements on how the supplier participates in the crisis organization set up by RVO.

If the explicit risk analysis shows that availability (B), integrity (I) or confidentiality (V) results in a score of medium or higher, the following additional requirements apply:

8. The supplier can demonstrate that ISO-270179 is complied with.

9. The supplier applies encryption to the data. Encryption is used for data-in-rest, data-in-use and data-in-transit. Explicit agreements have been made with the supplier about management of the encryption keys.
10. An SLA must be concluded with the supplier with periodic reporting at least once every 4 months. The SLA reporting must at least pay attention to the following points: a) (serious) security incidents and their handling b) backups made and verification of these backups c) examination of log files and results from them d) use of diagnostic data and logs by third parties.

If there is a cloud application with which personal data is processed, the following additional requirement applies:

11. The supplier can demonstrate that it complies with ISO-2701810.

Schedule 3: Arrangements on Breaches involving Personal Data

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.

Among other things, the Contracting Authority will request the following information:

- details of its organisation (name of organisation, address, postal code, place of business, professional register or trade register registration);
- details of the person reporting the breach (name, position, email address, telephone number(s));
- details of the data breach (short summary of the incident in which there was a Breach of the security of Personal Data, the minimum and maximum number of Data Subjects to whom the Breach of the Personal Data pertains, a description of the group of Data Subjects to whom the Breach pertains, the moment that the Breach took place (exact date or period), the moment the breach was discovered);
- information on the nature of the Breach (reading, copying, alteration, deletion, destruction, theft);
- type of Personal Data (address details, telephone numbers, email addresses or other addresses for electronic communication, access or identification details, financial details, citizen service number, passport or copies of other identity documents, gender, data of birth and/or age, special personal data such as ethnicity, political views, ideological beliefs, trade union membership, genetic details, biometric identification, health, sexual life and criminal details);
- technical and organisational measures which have been taken to deal with the data breach and prevent further Breaches;
- technical security measures (whether the Personal Data were partially or fully encrypted, hashed or otherwise rendered incomprehensible or inaccessible to unauthorised persons at the time of the data breach and how the Personal Data were rendered incomprehensible or inaccessible).

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