Annex 6a – Draft Data Processing Agreement

Contents

Data Processing Agreement (ARVODI 2018)

Contract number: 202308058

The undersigned:

1. The State of the Netherlands, which has its seat in The Hague,
represented by the Minister of Economic Affairs and Climate Policy,
legally represented in this matter by
René van der Burg, Director of Core Processes EU, the Netherlands Enterprise Agency, 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 4(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(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 between the Contracting Authority and the Contractor [name] dated [date], reference number 202308058.

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 in 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 Other Party will erase the Personal Data or return it to the Contracting Authority, as instructed by the Contracting Authority. The Other Party will delete any copies, barring statutory rules to the contrary.
In cases where the Other Party is responsible for erasing and/or destroying copies of the data, the Other Party will inform the Contracting Authority as soon as this has been done.

10.2 The Parties may agree specific retention periods for individual Personal Data or specific categories of Personal Data. When the agreed retention period has elapsed, the Other Party erases or returns and deletes copies of the relevant Personal Data, unless statutory rules require the retention of said Personal Data.

10.3 The Other Party will erase the Personal Data within one week, following the expiry of the Contract, failing which it will be fined €100,- per day, up to a maximum of €2.500,-.

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.

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

The Hague, [date]	[place], [date]
For the Minister of Economic Affairs and Climate Policy, And commissioned by René van der Burg, Director of Core Processes EU, Netherlands Enterprise Agency,	For [Contractor] [Signatory's position]
Jan van Putten Teammanager IUC EZK	[signatory's name]

Schedule 1. Processing Personal Data

To be completed by the Contractor	
Name of the Processor, including contact details	
Contact details of the representative of the Processor	
Contact details of the Processor's DPO	
Name and contact details of subprocessors	
Will the data be transferred to one or more countries outside of the EU?	

To be completed by the Contracting Authority	
Name of the Controller, including contact details	the Netherlands Enterprise Agency Prinses Beatrixlaan 2 NL-2595 AL The Hague
Contact details of the representative of the Controller	René van der Burg, Director of Core Processes EU, rene.vanderburg@rvo.nl
Contact details of the Controller's DPO	PbFG@minezk.nl
The subject/nature and objective of the Processing	Identity and access management
The type of Personal Data	Account data and standard personal data
Description of the categories of Personal Data	Names and email addresses of RVO employees. Company registration number and application number of farmer
Description of the categories of Data Subjects	Account data
Description of the categories of recipients of Personal Data	RVO Functional Management
Location of data processing	Public Cloud

Appendix 2. Appropriate technical and organisational measures

RVO protects its information in accordance with ISO standard 27001-2017 and the BIO v1.0 (Baseline Informatiebeveiliging Overheid, https://www.bio-overheid.nl/media/1400/70463-rapport-bio-versie-104_digi.pdf). It expects of the Contractor the following technical and organisational security measures:

Requirement	Description
06.2.1	Mobile devices in use by Personnel must store data related to the Performance in encrypted form in conformity with the classification of these data by means of cryptographic applications, exclusively using algorithms and settings in conformity with the most recent version of the NCSC document Guidelines for Transport Layer Security (TLS).
07.2.2a	The Contractor must demonstrably give an operational guarantee that Personnel receives an education and training in the area of security awareness fitting with the type of duties to be fulfilled, and gets yearly additional training in which at a minimum personal responsibilities and specific security frameworks of the Contracting Authority are also covered.
07.3.1	The Contractor must demonstrably have an operationally guaranteed process for the definition of responsibilities and tasks related to information security for the Performance, and must inform the Personnel that: 1. these remain in force after ending or changing the employment; 2. these must be executed.
08.2.1	The Contractor must demonstrably have an operational guarantee that all the information involved in the Performance is classified, and that the corresponding security measures will be adhered to.
08.3.x	The Contractor must have operationally guaranteed processes for the safe removal of media, the transport of media and the management of removable media that is involved in the Performance, in concordance with the classification scheme of the Contractor.
09.1.1	The Contractor must have an operationally guaranteed procedure for acquiring physical or logical access to information-processing facilities, including the issuing and revoking of accounts and authorisations, and a current registration thereof.
09.2.x	The Contractor must evaluate and update both the physical and logical access rights to information-processing facilities of the Personnel at least once a year via an operationally guaranteed and formal process, and produce immediate proof hereof any time the Contracting Authority requests it.
09.3.1	The Contractor must request from the Personnel that they adhere to the Policy for password use when using the authentication data related to the Performance.
10.1.x	If the Contractor is contractually or legally obligated to employ cryptography to protect data involved in the Performance, the Contractor must have policy and operationally guaranteed processes for the use of these cryptographic management measures in order to safeguard data and to protect their use. This policy and these processes also comprise the validity period of the measures and the corresponding cryptographic keys. This policy and these processes are strictly adhered to and immediate proof hereof is to be immediately provided any time the Contracting Authority requests it.
11.2.7	The Contractor immediately shows, any time the Contracting Authority requests it, that it has and works according to an operationally guaranteed process for the destruction of data on media when removing or replacing (parts of) Information Systems that contain these media and are involved in the Performance.
11.2.8	The Contractor immediately shows, any time the Contracting Authority requests it, that it has and works according to operationally guaranteed procedures for the protection of unmanaged Information Systems that are involved in the Performance.
12.2.1	The Contractor immediately shows, any time the Contracting Authority requests it, that it has and works according to operationally guaranteed processes for protection against malware on Information Systems involved in the Performance where at a minimum attention is paid to prevention, detection, communication and recovery.

13.2.1 The Contractor immediately shows, any time the Contracting Authority requests it, that it has and works according to operationally guaranteed policy rules, procedures and management measures for protection of the information transport involved in the Performance, which runs via all sorts of communication facilities.

14.1.2 Information Systems involved in the Performance that exchange information via public networks must use encrypted protocols for this at all times, with the used underlying encryption algorithms and settings established in conformity with the most recent version of the NCSC document 'Guidelines for Transport Layer Security (TLS)'.

18.1.3 The Contractor must demonstrably have operationally guaranteed procedures to protect against loss, destruction, forgery, unauthorised access and unauthorised release of registrations on Information Systems involved in the Performance, in conformity with legal, regulatory, contractual and company requirements.

18.1.CC-09 Data or programming of the Contracting Authority, including data present in it or generated by it, which includes metadata, that are on the Information Systems of the Contractor, are and remain at all times property of the Contracting Authority. Data that was given by the Contracting Authority to the Contractor can only be used by the Contractor for the purpose for which it was given. The Contracting Authority will take measures, including those for purposes of protection, to prevent perusing and irregular use by Personnel.

18.1.CC-10 The Contractor immediately shows, any time the Contracting Authority requests it, that it has and works according to operationally guaranteed processes for the destruction of data or programming of the Contracting Authority and all back-up media of the Contracting Authority. Both in the interim and after the contract ends, for any reason or for any cause, the Contracting Authority is authorised to order the Contractor to transfer the data to the Contracting Authority or to immediately destroy it.

18.1.CC-12 When data of the Contracting Authority are in the Information Systems of the Contractor, at the end of the contract between these two Parties the Contractor must provide assistance with the transfer of this information to the new supplier or back to the Contracting Authority, if the Contracting Authority so requests. Unless this is unacceptable by standards of reasonableness and fairness, the costs of the assistance are considered as part of the payments received by the Contractor for its Performances, regardless of how this is phrased.

18.1.CC-14 When data or programming of the Contracting Authority are in the Information Systems of the Contractor, any time the Contracting Authority requests it the Contractor must indicate where in the world these information system are located. If these are located outside the EU, this is only allowed in countries where a suitable level of data protection is offered; which countries these are is determined by the European Commission.

18.2.2 The Contractor must demonstrably have operationally guaranteed processes for the periodic assessment of the adherence to policy rules, norms and other requirements regarding security for Personnel involved in the Performance.

18.2.3 The Contractor must demonstrably have operationally guaranteed processes for the periodic assessment of the adherence to technical policy rules, norms and other requirements regarding security for Information Systems involved in the Performance.

- The Contractor must take additional measures on the basis of the risk involved in the Processing, as established on the basis of a Privacy Impact Assessment (PIA), for example. An overview of these measures is included below.

To be completed by the Contractor:

Certificates	**Organisational unit/service to which the certificate pertains**	**Term of validity of the certificate**	**Declaration of applicability**

Other qualifications

To be completed by the Contracting Authority:

Additional security requirements

Appendix 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 organisations (both businesses and government agencies) to report any serious data leaks to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) without delay. Under specific circumstances, they are obliged to report the data leak to the Data Subjects (the individuals whose Personal Data are involved in the leak) as well.

As the Contractor will be processing Personal Data within the framework of executing 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 leak for the Ministry of Economic Affairs and Climate Policy and the Ministry of Agriculture, Nature and Food Quality, 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 leak (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 leak 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 leak 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 leaks must be contacted without delay.

Examples of data leaks:

- 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 database 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 leaks
E:
T:
Availability:

To be completed by the Contracting Authority:

Contact details for data leaks
E: rvoinformatiebeveiliging@rvo.nl
T: NA
Availability: Working days from 07:30 to 18:30