Rijksdienst voor Ondernemend Nederland

Data processing agreement

Netherlands Enterprise Agency (*RVO*)-directorate Innovation and Entrepreneurship (*I&O*)- International Innovation & Cooperation Department - Team IRIS marktgerichte innovatie

/

[name Processor/Contractor]

Annex 3a – Draft Data processing agreement ARVODI-2025

Contract number: 202604115

The undersigned:

1. The State of the Netherlands, whose registered office is in The Hague,
hereby represented by the Minister of Economic Affairs and Climate Policy,
on behalf of these,
Ellen Jacobs, Director Innovation and Entrepreneurship, the Netherlands Enterprise Agency,
hereinafter referred to as: Client,

and

2. [full name and legal form of the Contractor],
(statutory) with its registered office in [...],
represented by
[name of signatory]
hereinafter referred to as: Contractor,

WHEREAS:

- insofar as the Contractor Processes Personal Data on behalf of the Client in the context of the Agreement, the Client qualifies as the Controller for the Processing of Personal Data and the Contractor as the Processor;
- insofar as an organization contracted by the Contractor Processes Personal Data on behalf of the Client in the context of the Agreement and the Contractor does not Processes Personal Data on behalf of the Client in the context of the Agreement, the Client qualifies as the Controller for the Processing of Personal Data and the organization contracted by Contractor as the Processor, in which case the Contractor guarantees and is responsible to the Client for ensuring that the Processor complies with the provisions below and from this point onwards in the Data processing agreement for Contractor the Processor will be read;
- The parties in this Data Processing Agreement, as referred to in Article 28, third paragraph, of the Regulation, wish to record their agreements about the Processing of Personal Data by the Contractor.

AGREE:

Article 1. Concepts

In this Data Processing Agreement, a number of terms are used with an initial capital letter. These terms have the meaning given to them in the ARVODI-2025 or the Regulation, on the understanding that a number of terms are focused on the Data Processing Agreement. Thus, and in addition thereto, the following terms, regardless of whether they are used in the plural or singular, or as a verb or noun, are understood in this Data Processing Agreement to mean:

1.1 ARVODI-2025: General Government Terms and Conditions for the Granting of Assignments to Perform Services 2025.

1.2 Person concerned: the person to whom Personal Data relates.

1.3 EEA: European Economic Area, i.e. all EU countries plus Liechtenstein, Norway and Iceland.

Vertrouwelijk

1.4 Personal Data Breach: a breach of security that accidentally or unlawfully leads to the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, data transmitted, stored or otherwise processed.

1.5 Recipient: a natural or legal person, public authority, agency or other body, whether a third party or not, to whom the Personal Data are disclosed. However, public authorities that may receive Personal Data in the context of a particular investigation in accordance with Union or Member State law do not qualify as Recipients; the Processing of such data by those public authorities is in accordance with the data protection rules applicable to the respective Processing purpose.

1.6 Agreement: the agreement between the Client and the Contractor named 'NL-UK bilateral quantum technology end-user engagement programme' of [date], with reference 202604115.

1.7 Personal data: all information about an identified or identifiable natural person that the Contractor Processes on behalf of the Client in the context of the Agreement.

1.8 Supervisory authority: an independent public authority 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 recitals and its appendices.

1.12 Processing: any operation or set of operations carried out under the Agreement on Personal Data, or a set of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasing or destroying data.

1.13 Data controller: a 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 may be identified or the criteria for its designation.

Article 2. Object of this Data Processing Agreement

2.1 This Data Processing Agreement regulates the Processing by the Contractor in the context of the Agreement and is inextricably linked to the Agreement.

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 described in Appendix 1.

2.3 The Contractor guarantees the application of appropriate technical and organizational measures to ensure that the Processing meets the requirements of the Regulation and the protection of the rights of the Data Subject is guaranteed.

2.4 The Contractor guarantees to comply with the requirements of the applicable laws and regulations regarding the Processing.

Article 3. Entry into force and duration

3.1 This Data Processing Agreement enters into force at the time it is signed by the Parties.

3.2 This Data Processing Agreement ends after the Contractor has erased and returned all Personal Data and has deleted existing copies with due observance of Article 10 of this Data Processing Agreement.

3.3 This Data Processing Agreement cannot be terminated prematurely.

Article 4. Scope of processing authority of the Contractor

4.1 The Contractor Processes the Personal Data exclusively on behalf of and on the basis of written instructions from the Client, unless a statutory provision applicable to the Contractor obliges the Contractor to Process. In that case, the Contractor will notify the Client of that legal provision prior to the Processing, unless that legal provision prohibits this notification for important reasons of public interest.

4.2 The Contractor has no control over the purpose of and the means of the Processing as referred to in the Regulation.

Article 5. Security of the Processing

5.1 Without prejudice to Article 2.3 of this Data Processing Agreement, the Contractor shall take the technical and organisational security measures as described in Appendix 2.

5.2 The parties acknowledge that ensuring an appropriate level of security may constantly force additional security measures to be taken. The Contractor guarantees a level of security appropriate to the risk.

5.3 Insofar as the Client expressly requests this in writing, the Contractor will take additional measures with a view to the security of the Personal Data.

5.4 The Contractor shall not Process Personal Data outside the EEA, unless it has obtained explicit written permission from the Client, if necessary accompanied by further conditions, and subject to deviating legal obligations.

5.5 The Contractor will inform the Client without unreasonable delay as soon as it has become aware of unlawful Processing of Personal Data or fails to comply with (the compliance with) technical and organisational security measures as referred to in the first and second paragraphs.

5.6 The Contractor shall assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the Regulation.

Article 6. Confidentiality by Contractor Personnel

6.1 The Personal Data are of a confidential nature as referred to in Article 11.1 of the ARVODI-2025.

6.2 The Contractor guarantees that its Personnel have undertaken to observe confidentiality as referred to in Article 11.2 of the ARVODI-2025.

Article 7. Sub-processor

If, with due observance of the provisions of Article 6 of the ARVODI-2025, the Contractor engages another Processor to perform processing activities on behalf of the Client, the same data protection obligations shall be imposed on this other Processor by means of an agreement as those included in this Processing Agreement.

Article 8. Assistance due to rights of the Data Subject

8.1 To the extent possible and taking into account the nature of the Processing by means of appropriate technical and organisational measures, the Contractor shall assist the Client in

fulfilling its duty to respond to requests for the exercise of the rights of the Data Subject as laid down in Chapter III of the Regulation.

8.2 The parties each bear the costs they themselves incur in connection with the first paragraph.

8.3 The Contractor will send a request from a Data Subject to the Client as soon as possible.

Article 9. Personal Data Breach

9.1 The Contractor will inform the Client without unreasonable delay as soon as it has become aware of a Personal Data Breach, in accordance with the agreements as laid down in Appendix 3.

9.2 The Contractor will also inform the Client about developments regarding the Personal Data Breach after a notification pursuant to the first paragraph.

9.3 The parties shall each bear the costs incurred by themselves in connection with the Personal Data Breach.

Article 10. Return or delete Personal Data

10.1 After the end of the Agreement, or as soon as agreed, the Contractor will ensure that, at the Client's choice, it deletes or returns all Personal Data to the Client and deletes existing copies, unless storage of the Personal Data is required by law.

10.2 The parties may agree on retention periods for individual or categories of Personal Data. After the agreed retention period has expired, the Contractor will ensure the deletion or return and the removal of copies of the Personal Data in question, unless the storage of this Personal Data is required by law.

10.3 Contractor deletes the Personal Data within 4 weeks after the end of the Agreement, or as soon as agreed, failing which the Contractor will owe a penalty of € 500 per day, with a maximum of the project value. Payment of the fine does not affect the obligations under Article 10 and the Contractor's obligation to compensate the damage resulting from the violation.

Article 11. Information obligation and audit

11.1 The Contractor will make all information available that is necessary to demonstrate that the obligations under this Data Processing Agreement have been and will be fulfilled.

11.2 The Client may carry out an audit of the processing activities covered by this Data Processing Agreement (or have it carried out) if concrete circumstances give cause to do so. The Contractor will fully cooperate with audits, including audits of Contractor Personnel, unless this cannot reasonably be expected of it.

11.3 The Contractor will immediately notify the Client if, in its opinion, an instruction from the Client in the context of Article 11, first and/or second paragraph of this Processing Agreement, constitutes a violation of a statutory provision on data protection.

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

11.5 The Client is at all times entitled to propose further measures in response to the information obtained on the basis of this article. The Contractor is obliged to implement these measures in a reasonable manner.

The Hague, [date]	[Location], [date]
FOR THE MINISTER/STATE SECRETARY OF ECONOMIC AFFAIRS AND CLIMATE POLICY on behalf of and commissioned by these Netherlands Enterprise Agency Directorate Innovation and Entrepreneurship Ellen Jacobs, director Innovation and Entrepreneurship on behalf of these,	FOR [CONTRACTOR/PARTY 2 AT ”THE UNDERSIGNED”],
E. Zandt, Team manager IUC EZK/LVVN	signatory’s name signatory’s position

Vertrouwelijk

Appendix 1. The Processing of Personal Data

In any case, this Annex shall specify:

To be completed by the Client (The Controller)	
Name of Controller including contact details	The Minister of Economic Affairs and Climate Policy, on behalf of these the Interim Director-General of the Netherlands Enterprise Agency (*RVO*): Mr. G.J.C.M. Bakker PO Box 93144, 2509 AC The Hague
Contact details of the Controller's representative	Directorate Innovation and Entrepreneurship Ellen Jacobs, director Innovation and Entrepreneurship PO Box 93144, 2509 AC The Hague
Contact details DPO of the Controller	Data Protection Officer of the Ministry of Economic Affairs and Climate Policy Bureau Bestuursraad PO Box 20401 2500 EK The Hague PbFG@minezk.nl
The subject/nature and purpose of the Processing	**Description of the processing activity:** The processing activities include collecting, receiving, accessing, consulting, recording, storing, updating and, where necessary, sharing personal data with authorised Contractor employees and, subject to Article 7, subcontractors, consultants and professional advisers who have a legitimate need to access such information for the performance of the Contract and/or the execution the Programme. Personal data may also be deleted in accordance with Article 10. **Purpose:** 1. Designing and delivering a coherent bilateral Netherlands-UK Quantum Technology End-User Engagement Programme (referred to as the "Programme") tailored to the needs, capabilities and potential application opportunities of the participating organisations; 2. Identifying and communicating with relevant individuals; 3. Providing the agreed services and managing the related business relationships.
The kinds (regular, sensitive, special, criminal, legal identification number), categories and types of Personal Data	**Regular personal data:** • Name (first name, last name, prefix, initials) • Nationality • Signature (of authorized signatories on requested documents in the context of the Programme) • Work-related details (job title and position, department, team, business email address, business phone number and website)

Vertrouwelijk

	• Communication data (email correspondence, chat messages, telephone notes, enquiries and complaints, questionnaires).
Description of categories Data subjects	- RVO employees/Client; - Employees of Netherlands Innovation Network; - Representatives of participating organisations (Quantum technology providers and End-users participating in the Programme); - Representatives of Quantum Technology ecosystem stakeholders involved in the Programme.
Description of (categories of) recipients of Personal Data	- RVO employees involved in the execution of the Programme; - Participating (NL and UK) organisations in the Programme, limited to the business contact details necessary for the Programme.
Location Processing Personal Data	Netherlands and/or United Kingdom – To be confirmed once Processor is known

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?	

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.

Appendix 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 Government Information Security Baseline (BIO) and BBN-2 may be replaced by ISO-27001.
- The Contractor implements additional measures based on the risk of the Processing, which have been determined, for example, as a result of a Data Protection Impact Assessment (DPIA). An overview of these measures is included below.

To be completed by the Contractor: <To be completed if the Contractor is known>

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

Other qualifications:

Additional security Requirements, to be completed by the Client:

<Optional, only applicable if there is a (new/extension) SaaS application>

The requirements, as stated in the Cloud Policy of the Netherlands Enterprise Agency (*RVO*), apply:

1. The supplier has a valid ISO-27001 or equal 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 (rvoinformatiebeveiliging@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.
8. 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:

9. The supplier can demonstrate that ISO-27017 is complied with.
10. 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.
11. An SLA must be concluded with the supplier with periodic reporting (frequency depends on risk profile). The SLA reporting must at least pay attention to the following points:

a) (serious) security incidents and their handling
b) security scans performed (pentest, vulnerability scan, etc.)
c) changes in third parties involved in the provision of services

This can be supplemented with the following topics:
d) backups made and verification of these backups
e) examination of log files and results from them
f) 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:

12. The supplier can demonstrate that it complies with ISO-27018.

Vertrouwelijk

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 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 Client 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 Client 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 Client'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 Client:

Contact details for data breaches
E: rvoinformatiebeveiliging@rvo.nl
Availability: Monday to Friday from 07:30 to 17:00 CET

Vertrouwelijk