Nucleaire Energie Organisatie Nederland

PERSONAL DATA PROCESSING AGREEMENT

NEO NL – COMPANY NAME

BY AND AMONG

1. **Nucleaire Energie Organisatie Nederland B.V.,** a company incorporated under the laws of the Netherlands, having its registered office in The Hague at (2596HP) Carel van Bylandtlaan 5, as registered with the Chamber of Commerce under number [99805480] (hereinafter to be referred to as: the **"Controller"**), duly represented by **.....**, in his/her role of **.....**,

and

2. [Fill in the name of the relevant entity], a company incorporated under the laws of [country], having its registered office in [town] at [address] and principal place of business in [city] at [address], as registered with the [Chamber of Commerce] under number [number] (hereinafter to be referred to as: the **"Processor"**) duly represented by [**Fill in representative name here**], in his/her role of [**Fill in role, e.g. CEO**].

Hereinafter individually **"Party"** and jointly **"Parties"**

HEREBY AGREE AS FOLLOWS:

1. Subject matter of this Data Processing Agreement

1.1. This Data Processing Agreement applies to all processing of Personal Data performed by the Processor subject to, or as a consequence of, the [name of agreement] of [date] between the parties for the [provision of services] (hereinafter to be referred to as: the "Main Agreement").

1.2. Capitalised terms such as "Processing", "Personal data", "Controller" and "Processor" have the meanings given to them in the GDPR (Regulation (EU) 2016/679). "Applicable Law" means all laws, regulations, regulatory requirements, binding guidance, codes of practice and other legally binding requirements (including case law) of the European Union and of any EU/EEA Member State applicable to a Party and/or the processing of Personal Data under this Data Processing Agreement, including laws relating to privacy, confidentiality, retention and security of personal data (including the GDPR), as amended or supplemented from time to time

1.3. The Processor processes Personal Data on behalf of the Controller pursuant to the Main Agreement. An overview of – inter alia - the categories of Personal Data, categories of data subjects, nature of the processing and purposes for which the Personal Data are being processed is provided in Annex 1.

2. The Controller and the Processor

2.1. The Processor processes Personal Data only on documented instructions from the Controller.

2.2. The Processor warrants that it will only process the Personal Data in such manner as - and to the extent that - this is necessary for, or otherwise in accordance with, the provision of the services under the Main Agreement, except as required to follow instructions of the Controller, or to comply with a legal obligation to which the Processor is subject (subject to Section 3.1). The Processor shall never process the Personal Data for its own purposes.

2.3. Processor will immediately inform Controller in writing if Processor is of the opinion that an instruction of Controller is in violation of, or causes a breach with this Data Processing Agreement or Applicable Law. Parties will together seek an appropriate solution in case any external developments endanger the lawfulness of the processing of the Personal Data.

2.4. When processing the Personal Data, the Processor warrants that it complies with Applicable Law and applicable instructions and regulations of competent public authorities.

2.5 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR (Articles 12–22).

2.6 The Processor shall, taking into account the nature of processing and the information available to the Processor, assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, including (as applicable) security of processing, breach notification, data protection impact assessments and prior consultation with supervisory authorities. The Processor shall maintain a record of processing activities as required by Article 30(2) GDPR and shall make such record available to the Controller upon request to the extent relating to the services under the Main Agreement.

3. Confidentiality

3.1. Without prejudice and in addition to any existing contractual arrangements between the Parties, the Processor warrants that it shall treat all Personal Data, the content of this Data Processing Agreement and notifications pursuant to Section 8 as strictly confidential towards any third parties, including public authorities, except as required to follow instructions of the Controller, or to comply with a legal obligation to which the Processor is subject, in which case the Processor will notify the Controller of such legal obligation, unless notification is prohibited due to reasons of general interests.

3.2. Processor shall take steps to ensure that natural persons acting under its authority and whom have access to the Personal Data act in accordance with this Data Processing Agreement and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1. The Processor shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing of the Personal Data. The Processor shall take these measures as specified in Annex 2 before the processing of Personal Data commences, and shall maintain these throughout the term of this Data Processing Agreement, or until the Processor has deleted or returned all Personal Data in accordance with Section 9, whichever is later.

4.2 The Processor shall not materially decrease the level of security described in Annex 2 during the term of this Data Processing Agreement. The Processor shall notify the Controller without undue delay of any material changes to the technical and organisational measures set out in Annex 2.

5. Information and Audit

5.1. At the request of the Controller, acting reasonably, the Processor shall promptly provide all information deemed necessary by the Controller for the Controller to comply with its obligations under Applicable Law.

5.2. The audit right of Controller under this Section 5 includes the right to perform an audit of the Processor in order to determine to what extent the Processor complies with the provisions of the Data Processing Agreement. Such audit will be performed by an independent third party and will take place at a time defined by both parties together, at the latest two months after the initial request of the Controller.

The Processor shall cooperate with the audit and provide the auditor reasonable assistance and access to the facilities, personnel, policies and documents that are necessary for the purpose of the audit. Notwithstanding the foregoing, where (i) a Personal Data Breach has occurred or is reasonably suspected, (ii) the Controller has a substantiated indication of non-compliance, or (iii) the Controller is required to respond within a shorter timeframe to a competent supervisory authority or other competent authority, the audit shall take place as soon as reasonably practicable and the Processor shall not unreasonably withhold agreement on timing. The Processor may propose, and the Controller shall reasonably consider, less intrusive audit measures (such as a desk audit, provision of relevant certifications and third-party audit reports, and targeted evidence) provided that such measures enable the Controller to verify compliance with this Data Processing Agreement.

5.3. The Controller will bear the costs for the audit, unless the audit shows that the Processor does not comply with the Data Processing Agreement. In such case, the Processor bears the costs of the audit, which includes all the fees of the third party auditor and the reasonable specified internal costs made by Controller.

6. International Data Transfers

6.1. The Processor shall notify the Controller of any (planned) transfers of Personal Data to a country outside of the European Economic Area, at the latest four weeks before commencing the transfer, in which event the Controller has the right at its discretion to object to such transfers within four weeks. The Controller may impose conditions on the transfer of Personal Data to a country outside the European Economic Area.

6.2. To the extent the processing of Personal Data involves a transfer of Personal Data from the EEA to a country outside the EEA which is not subject to an adequacy decision under Article 45 GDPR, the Parties shall enter into and comply with the Standard Contractual Clauses (Controller-to-Processor) as adopted by the European Commission in Implementing Decision (EU) 2021/914 (Module Two), and, where applicable, Module Four (Processor-to-Controller) (the "SCCs"). The SCCs, including their Annexes, which are available **here**, are deemed executed by the Parties upon signature of this Data Processing Agreement and/or the Main Agreement (as applicable). The

Parties shall complete the SCC Annexes (including Annex I, II and, where applicable, III) consistently with Annex 1 and Annex 2 to this Data Processing Agreement.

6.3. If the Court of Justice of the European Union or a local supervisory authority or similar governmental authority determines that this Data Processing Agreement, including without limitation the SCCs, is not a lawful method to facilitate transfers of Personal Data outside of the European Economic Area, the Parties shall negotiate in good faith an alternative method to facilitate such transfers.

6.4. Annex 1 sets out the transfers of Personal Data outside the European Economic Area (if any) upon the conclusion of tis Data Processing Agreement.

6.5 Upon the Controller's reasonable request, the Processor shall provide information and cooperation reasonably necessary for the Controller to carry out and document any transfer impact assessment and to implement supplementary measures where required. The Processor shall (i) notify the Controller of any legally binding request for disclosure of Personal Data by a public authority relating to the services, unless prohibited by law, (ii) challenge such requests where there are reasonable grounds to do so, and (iii) disclose only the minimum amount of Personal Data legally required.

7. Sub-Processors

7.1. The Controller provides the Processor with general authorization to engage sub-processors.

7.2. The Processor shall inform the Controller in advance of the engagement and/or replacement of a sub-processor, in which event Controller has the right at its discretion to object to (the engagement of) that sub-processor within four weeks.

7.3. The Processor shall remain fully liable vis-à-vis the Controller for the performance of – or the failure to perform – the obligations set out in this Data Processing Agreement by sub-processors, including under Section 10.

7.4. The Processor shall ensure that the sub-processor is bound in writing by the same obligations as the Processor under this Data Processing Agreement, and shall supervise compliance thereof. Processor shall, at the Controller's first request, provide a copy of such written agreement with the sub-processor.

8. Notification Obligations

8.1. In case of a data breach or another event set out in this Section, the Processor shall immediately notify the Controller, cooperate with the Controller and follow the Controller's instructions, in order to enable the Controller to perform a thorough investigation, to formulate a correct response and to take suitable further steps. Specifically, the Processor warrants that it provides the Controller with all information necessary to fulfil its legal obligations, such as the obligation to notify data breaches under Articles 33 and 34 GDPR.

8.2. In case of any breach of the security and/or confidentiality as set out in Article 32 GDPR or Sections 3 and 4 of this Data Processing Agreement leading to the loss or any form of unlawful processing, including destruction, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place, the Processor notifies the Controller within 24 hours after discovery of the breach. Such notification includes: (i)

the nature of the breach; (ii) the date and time upon which the breach took place and was discovered; (iii) the categories and amount of data subjects affected by the breach; (iv) the categories of Personal Data and amount of Personal Data records involved with the breach; and (v) whether and, if so, which security measures – such as encryption – were taken to render the Personal Data incomprehensible or inaccessible to anyone without the authorization to access these data.

8.3. In case of an investigation into or seizure of the Personal Data by government officials with the Processor, or any indication that this is about to take place, the Processor notifies the Controller as soon as possible but in any case within 24 hours after discovery of the investigation or seizure.

8.4. If the Processor receives a complaint, inquiry or request from a data subject or a supervisory authority relating to the processing of Personal Data under the Main Agreement, the Processor shall notify the Controller without undue delay and in any event within forty-eight (48) hours, and shall not respond directly unless legally required or authorised by the Controller. The Processor shall provide reasonable assistance to enable the Controller to respond within applicable statutory deadlines.

9. Returning or Destruction of Personal Data

9.1. Unless retention is required by Applicable Law, the Processor shall, at the discretion of the Controller, destroy or return the Personal Data to the Controller upon expiration or termination of the Main Agreement, in the manner and format indicated by Controller (where applicable). Processor shall simultaneously destroy all existing copies of the Personal Data. In such event, the Processor shall ensure that all engaged sub-processors cooperate to return and/or destroy the Personal Data. Controller's audit right as stipulated in Section 5 extends to verify Processor's execution of its obligations under this Section.

10. Indemnity

10.1. The Processor indemnifies the Controller and holds the Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Controller as a result of or connected to a breach of this Data Processing Agreement by the Processor.

11. Duration and Termination

11.1. This Data Processing Agreement shall come into effect and expire simultaneously with the Main Agreement, or at such date as the Processor has deleted or returned all Personal Data in accordance with Section 9, whichever is later.

11.2. The Controller has the right to terminate the Main Agreement when the Parties do not succeed to find a solution upon the objection of the Controller pursuant to Section 6 or 7.

11.3. Termination, cancellation or expiration of this Data Processing Agreement shall not discharge the Processor from its obligations meant to survive the termination, cancellation or expiration of this Data Processing Agreement, including e.g. the obligations deriving from Section 3, 4, 5, 8, 9 and 10 of this Data Processing Agreement.

12. Miscellaneous

12.1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Main Agreement, the provisions of this Data Processing Agreement shall prevail. In the event of any inconsistency between this Data Processing Agreement and the SCCs, the SCCs shall prevail to the extent required for the purpose of international transfers.

12.2. Any notifications performed pursuant to this Data Processing Agreement by the Processor to the Controller, for instance the notifications pursuant to Section 6, 7 and 8, shall be addressed to the contact provided in Annex 1.

12.3. This Data Processing Agreement is governed by the laws of the Netherlands. Any disputes arising out of or in connection with this Data Processing Agreement shall be brought exclusively before the competent court of Amsterdam, without prejudice to the possibilities of appeal.

Signed for and on behalf of the **Controller** by	Signed for and on behalf of the **Processor** by
Name: tba Title: CEO NEO NL	Name: [Fill in representative name here] Title: [Fill in role, e.g. CEO].
Signature	Signature
Date: ____/____/20____	Date: ____/____/20____

Annex 1

Privacy contact information

Contact information of the Controller and Processor.

For the Controller: Ernesto Pravisano, Compliance Officer – *privacy@neonl.com*;

For the Processor: Name Surname, Role here – *email@email.com*.

Categories of data subjects processed by Processor

The categories of data subjects include:

- Employees
- Vendors and contractors, suppliers and business partners

Categories of Personal Data the Processor will process

The types of personal data processed include:

- Identification data (e.g. names, initials)
- Contact details (e.g. email addresses, phone numbers)
- Professional information (e.g. job titles, employer details)
- Administrative and document-related data (e.g. correspondence, contracts, reports)

Special Categories (Article 9 GDPR)

- *N.a.*

Criminal Data (Article 10 GDPR)

- [TO BE COMPLETED]

National Identifiers

- N.a.

Please note that processing of BSN and/or Article 10 GDPR data (criminal convictions and offences) is only permitted if explicitly instructed in writing by the Controller in Annex 1 and only to the extent the Controller confirms that such processing is lawful under Applicable Law. The Processor shall apply the additional safeguards described in Annex 2 (High-Risk Data Safeguards).

Nature of the processing

- The subject matter of the processing concerns the provision and use of a document management system (DMS) for the storage, organization, retrieval, and sharing of digital documents.
- The nature of the processing includes the collection, recording, structuring, storage, adaptation, retrieval, consultation, use, transmission, and deletion of personal data within the system.

Purpose of the Processing

The purpose of the processing is to enable efficient document management, including secure storage, version control, collaboration, compliance with legal obligations, and facilitation of business operations. This includes HR document management, vendor document management and engineering document management. Hosting and maintenance of the Controller's customer database

Retention periods

Personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- During the term of the Main Agreement plus a period of [30 / 60] days after termination to allow for data export; thereafter all Personal Data shall be deleted or returned
- Login logs and audit trails: retained for a rolling period of 12 months for security monitoring purposes

Transfers of Personal Data outside the European Economic Area

- Not alllowed

Annex 2

The implemented security measures shall specifically include:

Access security

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: users accounts are protected using strong passwords, access to Personal Data is granted only to individuals with a need to know for the performance of their role and access rights are evaluated periodically, logging of access to the Personal Data.

Data integrity

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: data is backed up regularly, changes to Personal Data are logged, data integrity is ensured using digital signatures or checksums and data input is validated.

Organisational security

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: the classification of information, providing information to the personnel with access to the Personal Data and disciplinary consequences.

Physical security

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: restricted access to physical storage location, surveillance of areas where the Personal Data are stored, prevention, detection and operating procedure in case of emergencies (such as fire, intrusion and water) and redundant systems.

Network and data security

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: using firewalls, by employing and constantly updating antivirus software, encryption and pseudonymization of the Personal Data during transfer and storage, using secure communications channels and employing an intrusion detection and prevention system.

Security incident management

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: incident response training and developing a security incident plan and business continuity plan.

Testing and evaluation procedures

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: procedures to evaluate and improve the effectiveness of the security measures, such as an independent external audit cycle and certifying for relevant security standards.

Data disposal

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: Personal Data is irretrievable deleted when no longer necessary and discarded storage hardware is wiped in accordance with industry practice.

High-Risk Data Safeguards (BSN / Article 9 / Article 10)

Please specify: [TO BE INSERTED BY PROCESSOR]

For example: where the Processor processes special categories of data, BSN or Article 10 data, the Processor shall implement enhanced measures, including: (i) strict role-based access control with least privilege and MFA; (ii) separate logging/monitoring of privileged access; (iii) encryption in transit and at rest with documented key management; (iv) segregation of such datasets where feasible; (v) stricter retention and deletion controls; and (vi) documented procedures