ANNEX I – DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") shall form part of the Accession Agreement and its appendices hereto between EFETnet and the Customer concerning services provided by EFETnet for Customer (the "**Agreement**"). This DPA is entered into by and between the Customer ("**Controller**") and EFETnet ("**Processor**").

The Controller and Processor are hereinafter also referred to collectively as "**Parties**" and individually as "**Party**."

Within the scope of its business activities and in accordance with the further provisions contained in the relevant Agreement, the Processor shall receive from the Controller personal data for which the latter is responsible. The Parties are agreeing on the provisions set forth in this DPA in order to fulfill the Controller's obligations pursuant to European data protection law.

1. Definitions

1.1 "Personal data" means all information concerning an identified or identifiable natural person ("**Data Subject**"). A natural person is considered to be identifiable if he/she can be identified directly or indirectly, particularly by means of attribution to an identifier such as a name, an ID number, location data, an online ID, or one or more particular features that are an expression of the physical, physiological, genetic, mental, financial, cultural, or social identity of this natural person (hereinafter "**Data**").

1.2 "Commissioned data processing" means the collection, processing, or use of Data by the Processor on behalf of the Controller.

2. Subject matter and content of contract

2.1 Subject matter and term of contract

The subject matter of the contract is described in the Agreement.

The term of the DPA is geared toward the term of the Agreement. This DPA shall terminate upon the end of the Agreement.

2.2 Nature of Data

(a) The data processed by Processor on behalf of the Controller may include to a certain extent Data of Controller, referring to employees, customers and contact persons of Controller.

(b) While Processor will perform any additional hosting and maintenance services to the Controller, additional Data may be affected, in particular user login data of the users of the services provided by the Processor.

2.3 Purpose of collection, processing, or use of Data

The purpose of the collection, processing, or use of the Data is described in further detail in the Agreement.

User-log-ins of users of the Controller shall exclusively be used for the technical provision of the services and shall only be processed by the Processor for the purpose of technical provision of the services.

2.4 Nature and scope of collection, processing, or use of Data

The nature and scope of the collection, processing, or use of the Data is described in further detail in the Agreement.

User-log-ins of users of the Controller shall be collected and stored by Processor as a service provider and shall be deleted after termination of the respective agreement.

2.5 Category of Data Subjects

(a) Employees, customers and and/or contact persons related to Controller.

(b) Workers (employees and freelance contractors as well as temporary employees) of the Controller.

2.6 Technical and organizational measures

The technical and organizational measures to be implemented by the Processor are provided for in Annex A to this DPA.

2.7 Correction, erasure, and blocking of Data; right of objection and of portability of Data

(a) The rights of the Data Subjects concerned in the Processor’s handling of Data, particularly the rights to correction, erasure, and blocking of Data, the right to data portability and the right to object, shall be asserted vis-à-vis the Controller. The Controller bears sole responsibility for safeguarding these rights.

(b) The Processor will forward to the Controller in due time for proper handling any inquiries the Processor may receive from Data Subjects within the scope of the former’s activities on behalf of the Controller. The Processor is not entitled to answer these inquiries independently without consulting the Controller.

(c) The Processor will correct, block, and/or erase Data on the Controller’s instructions within reasonable time.

2.8 Obligations of the Processor

(a) The Processor may process Data only within the scope of the Agreement and the documented instructions issued by the Controller, including with regard to transfers of Data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) The Processor must check and document compliance with the technical and organizational measures within the meaning of Sec. 2.6 of this DPA at reasonably regular intervals. The Processor must present the report to the Controller accordingly.

(c) The Processor is responsible for ensuring confidentiality. Persons on the Processor’s side who are authorized to access the Controller’s Data must undertake an obligation to maintain confidentiality or be subject to an appropriate statutory duty of confidentiality, and must be instructed as to the particular data protection obligations arising from this DPA and the existing instructions and designations of specific purposes.

2.9 Establishment of subcontracting relationships

(a) The Processor shall be allowed by the Controller to appoint other data processors within the scope of this DPA. The Processor will inform the Controller of any changes with regard to the use or replacement of other processors with reasonable prior notice.

(b) In the event that the Processor contracts with other processors, the Processor must ensure by way of contractual provisions that the provisions agreed by and between the Controller and the Processor also apply accordingly vis-à-vis the other processors. In particular, other processors are required to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the General Data Protection Regulation.

(c) The Processor must check, in advance and regularly during the term of the subcontracting relationship, the necessary technical and organizational measures taken by the other processor to protect the Data. Forwarding of Data is only permissible if the other processor has implemented the necessary technical and organizational measures in accordance with the provisions of this DPA.

(d) Where that other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

2.10 Rights of control by the Controller

The Processor accepts and agrees that the Controller is entitled to review compliance with the applicable data protection provisions and this DPA during the usual business hours on cost of the Controller. The Processor agrees to provide the Controller, within a reasonable period, with all information that is reasonably necessary in order to perform such checks. To the extent that, in the Controller’s view, an audit on site at the Processor’s premises is necessary, the Processor will provide the Controller with access to the Processor’s office space and the right to inspect the stored Data and the data processing programs on premise. The Controller is entitled to have this review performed by a third party (auditor) to be designated in the individual case. The Controller must announce the performance of such an audit in writing at least thirty (30) working days in advance and shall in full bear the costs of the Processor in this regard, including the costs of personal which will support the Controller on premise. To the extent permitted under applicable law, the review of compliance with the applicable data protection provisions and this DPA can be performed by an independent auditor appointed by the Processor.

The Processor will provide the Controller on request with the report of the independent auditor. The Controller shall bear the costs for appointment of the independent auditor pro rata.

2.11 Notices in the case of violations by the Processor

(a) The Processor shall notify the Controller without undue delay, and in any event within twenty-four (24) hours after the relevant determination, of all cases in which violations of the provisions to protect the Controller’s Data or of the stipulations set down in this Commissioned Data Processing Annex have been committed by the Processor or any persons employed by it.

(b) All incidents in which Data have been lost or have been transmitted or obtained by third parties without authorization must be reported to the Controller regardless of the cause. The Processor must, in consultation with the Controller, take appropriate measures to secure the Data and to mitigate possible adverse consequences for Data Subjects. To the extent that the Controller is under obligations of notification, the Processor must support the Controller in fulfilling such obligations.

2.12 Assistance obligations of the Processor

The Processor is obligated to assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

The Processor is further obligated to assist the controller in ensuring compliance with the Controller’s obligations pursuant to Articles 32 to 36 GDPR. In particular, this applies to data protection impact assessments, within the scope of prior consultations with data protection authorities, to the reporting of data protection violations to data protection authorities and to the communication of personal data breaches to the data subject. Notably, the Processor is obligated to notify the Controller within 24 hours of violations of provisions protecting personal data or of specifications stated in this Appendix committed by the Processor itself or by persons employed by the Processor.

The Controller shall reimburse the Processor for any costs arising of or in connection with the support of the Controller as set out herein.

2.13 Instructions from the Controller

(a) The processing of the Controller’s Data by the Processor shall take place exclusively within the scope of this DPA and the specific documented individual instructions issued by the Controller.

(b) The Processor is required to follow (individual) instructions regarding the nature, scope and procedures used for data processing.

(c) The Processor shall notify the Controller without undue delay if the Processor believes any instructions issued by the Controller violate the provisions of data protection law. The Processor is entitled to suspend its implementation of the instructions in question until such time as a responsible person within the Controller’s organization confirms or amends them.

2.14 Erasure after the termination of the commission

After the conclusion of the contractual work, the Processor must turn over to the Controller any and all Data that it has processed for the Controller or must, with the prior consent of the Controller, destroy such Data in a manner compliant with data protection or securely erase them in accordance with the state of the art. A right of retention with regard to the documents, Data, results of processing and use, and the relevant data storage media is ruled out except to the extent that storage of the Data is required under the laws of the European Union or of an EU Member State.

3. Further obligations of the Processor

3.1 The Processor shall not use the Data provided for data processing for any other purposes. Copies or duplicates must not be made without the Controller’s knowledge unless this is owed in accordance with the services commissioned in this DPA. The Processor warrants that the Data it processes for the Controller will be logically separated from other data stocks.

3.2 Controller will remunerate the Processor in accordance with the applicable price list of Processor for the following support services as set out herein:

(a) The Processor shall support the Controller within a reasonable scope in defending itself against claims based on alleged or actual violation of the requirements of data protection law. The Controller, for its part, shall follow up on complaints from

Data Subjects within the scope of the Controller's responsibilities under data protection law in an appropriate form and shall handle complaints from Data Subjects.

(b) The Processor acknowledges that notices to Data Subjects based on a claim to information will be issued exclusively by the Controller or by a party authorized and empowered by the Controller. The Processor is obligated to provide the Controller with the information necessary to this end and to support the Controller.

(c) The Processor is required to support the Controller in preparing necessary records of processing activities, to the extent required.

(d) The Processor shall support the Controller in performing data protection impact assessments if one type of processing is expected to result in a high risk to the rights and freedoms of natural persons.

(e) The Processor agrees to notify the Controller of the results of reviews conducted by the data protection supervisory authorities without undue delay to the extent that these are related to this DPA. The Processor shall inform the Controller of any complaints issued by the data protection supervisory authorities that concern the scope of the Processor's responsibility and shall solve any complaints that have been determined to the extent required by law.

4. Obligations of the Controller

4.1 Solely the Controller is responsible for the admissibility of the processing of Data and for safeguarding the rights of the Data Subjects.

4.2 The Controller is required to inform the Processor without undue delay and in full if, during its review, it discovers any errors or irregularities in the processing of the Data by the Processor.

4.3 Controller shall indemnify and hold harmless Processor from any claims of third parties while performing the duties and processing activities in scope of the DPA unless the Processor has given cause for the claim due to an infringement of the provisions of this DPA.

5. Final provisions

5.1 If the Controller's Data at the Processor should be jeopardized by seizure or confiscation, by insolvency or composition proceedings or other events or third-party actions, the Processor shall inform the Controller. The Processor shall notify all third parties affected in this context without undue delay that the right of disposal and ownership of the Data rest exclusively with the Controller.

5.2 Should one or more provisions of this DPA be invalid, such circumstance shall not affect the validity of the remainder of the DPA. In the event that one or more provisions of the DPA is or are invalid, the Parties shall agree on a legally valid substitute provision that most closely approximates the invalid provision in economic terms. The same applies in the event that there should be a gap in the provisions hereof..

5.3 In the event of any contradiction between this DPA and other contracts and agreements between the Parties, the provisions of this DPA shall take precedence.

Place, Date

Signature(s)

EFETnet	Customer:
Name: (H. Brunswick)	Name (s):
Function: Managing Director	Function:

ANNEX A TO DPA

Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation, and the nature, scope, circumstances, and purposes of processing as well as the varying likelihood of materialization and severity of the risk to the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures in order to ensure a level of protection appropriate to the risk; these measures include, but are not limited to, the following to the extent appropriate:

- pseudonymization and encryption of the Data;

- the ability to ensure the confidentiality, integrity, availability, and ability to withstand strain of the systems and Services on an ongoing basis in connection with the processing;

- the ability to restore the availability of the Data and access thereto swiftly in the event of a physical or technical incident; and

- a procedure for regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing.

Notwithstanding the foregoing, the following specific measures shall be taken:

1. Physical access control

Measures to deny unauthorized persons physical access to the data processing systems and equipment with which the Data are processed:

The processor shall secure access to its premises by using keys and by using an access application (KISI) during day time, so that only authorized individuals have access. Accounts shall be able to be disabled individually, additionally access shall be protocolled

All data is held at a secure data center which has appropriate controls in place.

2. Systems access control

Measures that prevent unauthorized persons from using the data processing systems, equipment, and procedures:

All system access through the GUI of the CMS Software System is via secured application web pages. All administration access is via two-factor authentication. All system access on the database level needs to be authorized. All system access on the database level is logged and periodically reviewed against authorisations.

3. Data access control

Measures that ensure that the parties authorized to use the data processing procedures can only access the Data to which their access authorization applies:

All system access is via secured application web pages. All administration access is via two-factor authentication. All server side access to databases is limited, password protected and system audited.

4. Transmission control

Measures that ensure that the Data cannot be cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of the Data by means of data transmission facilities is envisaged.

Access to the systems is via secured web access (HTTPS). All data transferred system to system is encrypted using strong PKI encryption (ebXML MS 2.0).

5. Input control

Measures that ensure that it is possible to check and establish after the fact whether and by whom Data have been input into IT systems, modified or removed.

All CMS data transaction is subject to system auditing. All database input are journaled.

6. Job control

Measures that ensure that, in the case of commissioned processing of Data, the Data can only be processed in accordance with the instructions of the Controller.

Performance of a formal process of placing the order; the Processor shall verify and document the security measures taken by its subcontractors.

Managed according to procedures set out in the terms of operation of EFETnet and its sub-contractors as governed by standards such as ISO27001

7. Availability control

Measures that ensure that Data is protected from accidental destruction and/or loss.

Managed according to procedures set out in the terms of operation of EFETnet and its sub-contractors as governed by standards such as ISO27001.

8. Separation control

Measures that ensure that the Data collected for different purposes can be processed separately.

Logical separation of the individual data sets for each of the Processor’s controllers.

Systems are designed and build to provide multiple users and multiple Customer. All Customer data is logically separated through database views and accessed via individual accounts which are subject to a strict user access rights mechanism allowing administration users to manage the access rights of other accounts to data and functions.