DATA PROCESSING ADDENDUM TO SOFTWARE AS A SERVICE AGREEMENT

This Data Processing Addendum to the Software as a Service Agreement including Sub-appendix 1 – Instructions for the Processing of Personal Data and Sub-appendix 2 – List of Approved Sub-processors (this "DPA") is made and entered into on the Effective Date of the Software as a Service Agreement ("SaaS Agreement") by and between;

(1) the data controller; the Customer stated in the SaaS Agreement ("Customer" or "Controller"); and

(2) the data processor; the supplier Mevisio stated in the SaaS Agreement ("Mevisio" or "Processor").

The parties have concluded an agreement on the provision of the software platform that goes under the brand Mevisio and the relevant support services ("Services") which involves the processing of Controller's personal data on behalf of Controller for the duration of the SaaS Agreement.

In the event of any contradiction between this DPA and the provisions of the SaaS Agreement entered into between the parties, this DPA shall prevail.

1 BACKGROUND

1.1 The Parties have concluded the SaaS Agreement on the provision of the software platform that goes under the brand Mevisio and the relevant support services ("Services"). Within the undertakings arising from the SaaS Agreement when the Data Processor provides the Services, the Data Processor might process personal data on behalf of the Data Controller. This DPA governs the rights and obligations of the Data Controller and the Data Processor when the Data Processor processes personal data on behalf of the Data Controller, pursuant to the SaaS Agreement.

1.2 In the event of any contradiction between this DPA and the provisions of the SaaS Agreement entered into between the parties, this DPA shall prevail in relation to rights and obligations related to the processing of personal data. In the event of any contradictions between this DPA and the Data Controller's documented instruction, this document shall take precedence, unless otherwise specifically stipulated or clearly indicated by the circumstances.

1.3 This DPA aims to meet the current requirements for a DPA in accordance with Applicable Data Protection Legislation.

2 DEFINITIONS

The terms used in this DPA are defined in this section or directly in the sections where the terms are used. Where terms defined in the GDPR (as defined below) are used, those terms shall have the same meaning as in the GDPR, unless otherwise specified. Any capitalized terms utilized within this DPA, yet not expressly defined herein, shall carry the meaning ascribed to them in the SaaS Agreement.

2.1 "Applicable Data Protection Legislation" means all privacy, data protection and personal data laws of the European Union or a member state of the European Union applicable to the personal data processing that is carried out under this DPA.

"Data Controller" has the meaning set forth in the recitals.

“Data Processor” has the meaning set forth in the recitals.

“DPA” has the meaning set forth in the recitals.

“GDPR” 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).

“SaaS Agreement” has the meaning set forth in the recitals.

"Party" and "Parties” has the meaning set forth in the SaaS Agreement.

“SCC” means the standard contractual clauses for the transfer of personal data to data processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, implemented by the European Commission decision (EU) 2021/914 of 4 June 2021.

“Sub-processor” means the legal person who is engaged by the Data Processor to carry out specific processing activities on behalf of the Data Controller.

“Sub-processor Notice” has the meaning set forth in Section 8.3.

3 OBLIGATIONS OF THE DATA CONTROLLER

3.1 The Data Controller undertakes to ensure that there is a legal basis for the processing and for compiling correct instructions with regard to the nature of the processing so that the Data Processor and any Sub-processor can fulfill their obligations according to this DPA and the SaaS Agreement, where applicable.

3.2 If the Data Controller intends to process special categories of personal data (sensitive personal data) in the Services, the Data Controller shall inform the Data Processor in advance before the special categories of personal data is added to the Service, and the Data Controller shall also ensure that it follows from a Data Controller's Instructions to the Data Processor.

3.3 The Data Controller shall, without undue delay, inform the Data Processor of changes in the processing which affect the Data Processor's obligations pursuant to Applicable Data Protection Legislation.

3.4 The Data Controller is responsible for informing data subjects, whose personal data is subject to processing under this DPA, about the processing and safeguard the rights of data subjects in accordance with Applicable Data Protection Legislation, as well as to take every other measure required of the Data Controller pursuant to Applicable Data Protection Legislation.

4 PROCESSING OF PERSONAL DATA

4.1 The Data Processor shall ensure compliance with Applicable Data Protection Legislation as well as its obligations under this DPA when processing personal data on behalf of the Data Controller.

4.2 The Data Processor may only process personal data on behalf of the Data Controller in accordance with the Data Controller’s documented instructions, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by the laws of the European Union or a member state of the European Union to which the Data Processor is subject, in which case the Data

Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.3 The Data Controller's initial instructions are set out in this DPA and Sub-appendix 1 – Instructions for the Processing of Personal Data. Subsequent instructions may also be given by the Data Controller throughout the duration of the processing of personal data. These instructions shall always be documented. The Data Controller has an obligation to ensure that the Data Processor has received the instructions communicated by the Data Controller and shall, in consultation with the Data Processor, consider whether an update of the instructions requiring the Data Processor to take additional measures can be implemented. The Data Processor shall, if a subsequent instruction involves a certain change and the instruction does not result from obligations under Applicable Data Protection Legislation, be given a reasonable time to implement such an update.

4.4 In the event of an update of the instruction that goes beyond the obligations arising from Applicable Data Protection Legislation, the Data Processor shall be entitled to compensation for documented additional costs.

4.5 The Data Processor has the right to terminate the SaaS Agreement, including this DPA, according to Section 14.3 if an update of the instruction goes beyond the obligations arising from Applicable Data Protection Legislation and/or the Data Processor is unable to carry out/implement the requested update, or if it would involve a significant change or additional cost. The aforementioned only applies if the Data Controller does not choose to recall an update of the instruction.

4.6 In the event that a Data Controller adds special categories of personal data to the Service without providing Instructions in accordance with Section 3.2, the Data Processor is entitled to terminate the SaaS Agreement according to Section 14.3. The Data Processor also has the right to terminate the SaaS Agreement in accordance with Section 6.4 if the Data Processor considers that it cannot ensure an appropriate level of security for the special categories of personal data.

4.7 The Data Processor shall immediately inform the Data Controller if, in its opinion, the Data Processor has not received sufficient instructions to process personal data in accordance with its obligations pursuant to the SaaS Agreement or if, in the Data Processor's opinion, an instruction infringes Applicable Data Protection Legislation, and defer the processing until further instructions from the Data Controller are provided.

4.8 If the Data Controller persists with an instruction which, in the Data Processor's opinion, infringes Applicable Data Protection Legislation pursuant to Section 4.7, the Data Processor shall have the right to terminate the SaaS Agreement, including this DPA, according to Section 14.3 .

4.9 The Data Processor shall, without undue delay, inform the Data Controller about technical, organizational, or financial changes, including changes in the ownership, which are likely to affect the Data Processor's capability of complying with its obligations in accordance with this DPA.

5 THE DATA PROCESSOR'S OBLIGATIONS TO ASSIST THE DATA CONTROLLER

5.1 The Data Processor shall assist the Data Controller in fulfilling its obligations in accordance with Applicable Data Protection Legislation per the Data Controllers request. This means that the Data Processor shall:

a) through appropriate technical and organizational measures, to the extent possible and with due regard to the nature of the processing, assist the Data Controller in fulfilling the Data Controller's obligations to respond to requests for exercising the data subjects right laid down in Chapter III of the GDPR (such as

rectification, deletion, restriction, data portability and request of access);

b) assist the Data Controller in fulfilling the Data Controller's obligations to take appropriate security measures for the processing of personal data under this DPA to ensure a level of security appropriate considering the level of risk which the processing of personal data in question entails in accordance with Article 32 of the GDPR;

c) assist the Data Controller by providing the information, assistance and resources that are reasonably necessary for fulfilling the Data Controller's obligation to report personal data breaches to the competent supervisory authority in accordance with Article 33 of the GDPR;

d) assist the Data Controller with the information, assistance and resources that may reasonably be required to fulfill the Data Controller's obligation to inform the data subject, within the framework of this DPA, in the event of a data breach that is likely to result in a high risk to the rights and freedoms of natural persons in accordance with Article 34 of the GDPR;

e) assist the Data Controller in fulfilling the Data Controller's obligation to carry out data protection impact assessments for processing under this DPA, which is likely to result in a high risk to the rights and freedoms of individuals in accordance with Article 35 of the GDPR; and

f) assist the Data Controller by providing the Data Controller with the information, assistance and resources that may reasonably be required to fulfill the Data Controller's obligation to provide information and documentation to the supervisory authority for prior consultation, and when necessary, and to a reasonable extent, attend meetings with the supervisory authority in accordance with Article 36 of the GDPR.

5.2 When the Data Processor assists the Data Controller in fulfilling the Data Controller's obligations under Applicable Data Protection Legislation in accordance with Sections 5.1 b) – f) above, consideration shall be given to the type of processing it refers to, and the information available to the Data Processor. In order to avoid any misunderstandings, nothing in this section shall be interpreted as indicating that the Data Processor may act on behalf of the Data Controller. The Data Processor may only act to fulfill its obligations vis-à-vis the Data Controller.

6 SECURITY AND CONFIDENTIALITY

6.1 The Data Processor undertakes to take all appropriate technical and organizational measures to protect the personal data being processed under this DPA in accordance with Applicable Data Protection Legislation and in particular Article 32 of the GDPR. The Data Processor shall ensure that its Service fulfills the requirements of the principles of privacy by design and privacy by default in line with Applicable Data Protection Legislation as set out in the SaaS Agreement and this DPA.

6.2 The Data Processor has implemented the technical and organizational measures set out in the instructions from the Data Controller and undertakes not to substantially change these or otherwise change the security measures in a way that results in a lower level of security than the one intended in Section 6.1 and the Data Controller's instructions.

6.3 The Data Processor is entitled to compensation for additional costs and has the right to increase the price of the Services due to the need to implement additional security measures for the processing of special categories of personal data.

6.4 In the event that the Data Processor considers that an appropriate level of security cannot be maintained when processing special categories of personal data, the Data Processor shall inform the Data Controller and the Data Processor is entitled to terminate the SaaS Agreement according to Section 14.3 with immediate effect.

6.5 The Data Processor is obliged to immediately inform the Data Controller if the Data Processor considers that the implemented security measures no longer comply with the requirements set out in the Applicable Data Protection Legislation and wait for further instructions from the Data Controller.

6.6 The Data Processor shall ensure that only its employees, and other persons carrying out work under the Data Processor's supervision, and who must have access to the personal data in order to fulfill the Data Processor's obligations under this DPA, will have access to such personal data. The Data Processor shall ensure that all such employees and other persons are bound by appropriate confidentiality obligations, either by law or by agreement. The Data Processor shall also ensure that they understand what confidentiality obligation entails and that such persons only process personal data in accordance with documented instructions from the Data Controller unless the person concerned is required to do so under Applicable Data Protection Legislation.

7 PERSONAL DATA BREACHES

7.1 The Data Processor shall without undue delay after the Data Processor having become aware of the personal data breach, notify the Data Controller.

7.2 A notification pursuant to Section 7.1 shall include all information which may reasonably be required by the Data Controller to fulfil its obligations under Applicable Data Protection Legislation. Such information includes e.g. a description of:

a) the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) likely consequences as a result of the data breach; and

d) the measures taken or proposed to be taken to rectify the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

7.3 Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information available and further information shall, as it becomes available, subsequently be provided without undue delay.

7.4 The Data Controller shall compensate the Data Processor for any direct costs that the Data Processor incurs if the measures taken under this Section 7 are due to the Data Controller's non-compliance of Applicable Data Protection Legislation.

7.5 The Data Processor is not entitled to inform any third parties, including data subjects, of the personal data breach without the Data Controller's prior written consent, unless required to do so by the laws of the European Union or a member state of the European Union to which the Data Processor is subject.

8 SUB-PROCESSORS

8.1 The Data Processor is aware that it must comply with the requirements specified in Article 28(2) and (4) of the GDPR in order to engage a Sub-processor.

8.2 A list of approved Sub-processors at the time of entering into this DPA is set forth in Sub-appendix 2 – List of Approved Sub-processors. The Data Processor shall, from time to time, maintain an updated list of the Sub-processors who have been approved by the Data Controller as well as the countries in which these Sub-processors perform their activities and other relevant information. At the Data Controller's request, the Data Processor shall submit a copy of the list to the Data Controller.

8.3 The Data Processor has the Data Controller's general written authorisation for the engagement of Sub-processors. The Data Processor shall inform the Data Controller in writing of any intended changes concerning the addition or replacement of Sub-processors ("Sub-processor Notice") at least thirty (30) days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned Sub-processor(s). A Sub-processor Notice to the Data Controller, to engage or replace a Sub-processor shall be in writing and as a minimum include the following information:

(i) company name;

(ii) company registration number (or equivalent);

(iii) address and country;

(iv) a description of the sub-processing; and

(v) where the personal data will be processed.

8.4 In the event the Data Controller informs the Data Processor within thirty (30) days after receiving the Sub-processor Notice from the Data Processor that the Data Controller does not approve of the use, addition or replacement of a Sub-processor, the Data Controller may terminate the SaaS Agreement including this DPA without penalty, however without the right to any repayment of paid or accrued fees. The Data Controller acknowledge that the Data Controller is entitled to such termination only to the extent the Data Controller can demonstrate that the Data Controller has reasonable grounds to assume that the Sub-processor will not process the personal data in accordance with the GDPR. If the Data Controller does not object on reasonable grounds within thirty (30) days from receiving the Sub-processor Notice, the Sub-processor is deemed to be approved by the Data Controller.

8.5 Where the Data Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Data Controller, the Data Processor shall enter into an agreement with the Sub-processor which imposes corresponding obligations as are applicable to the Data Processor in accordance with this DPA, and under which the Sub-processor also provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this DPA and Applicable Data Protection Legislation. The Data Processor shall therefore be responsible for requiring that the Sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to this DPA and Applicable Data Protection Legislation.

8.6 If the Sub-processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the Sub-processor.

9 TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

9.1 The Data Processor may transfer personal data on behalf of the Data Controller to a country outside of the EU/EEA (i.e., third country), provided such transfers meet the requirements and undertakings which follow from Applicable Data Protection Legislation and the Data Controller's instructions.

9.2 The Data Processor undertakes to enter into the relevant module of the SCCs with its Sub-processors which transfer personal data outside EU/EEA, unless another applicable transfer mechanism applies or if the transfer is based on an adequacy decision, and to take all reasonable measures to control that the engaged Sub-processors ensure the lawfulness of any further transfers of personal data that the Sub-processors' sub-processors may undertake.

9.3 The Data Processor shall inform the Data Controller, without undue delay, if an adequate level of protection can no longer be guaranteed for the transfer of personal data to, or access from, a country outside the EU/EEA, or if the transfer or processing can, in any other way, be considered contrary to the Applicable Data Protection Legislation. Furthermore, in such instances, the Data Processor shall immediately take steps to ensure that personal data can continue to be processed in accordance with Applicable Data Protection Legislation and inform the Data Controller of the measures taken.

10 REQUEST FOR INFORMATION AND DISCLOSURE OF PERSONAL DATA

10.1 In cases where a data subject or other third-party requests information from the Data Processor in respect of processing of personal data which is processed on behalf of the Data Controller, the Data Processor shall refer such data subject or third party to the Data Controller.

10.2 In the event a public authority requests the type of data as set forth in Section 10.1 above, the Data Processor shall immediately inform the Data Controller of the request, unless prevented by applicable European Union law or laws of a member state of the European Union, and the Data Processor and the Data Controller shall, in consultation, agree on a suitable course of action.

10.3 The Data Processor shall not disclose or make any personal data which is processed on behalf of the Data Controller available unless the Data Processor is under legal obligation deriving from laws of a member state of the European Union or European Union law, or court or public authorities' order to disclose the information (provided that such court or public authority is located within the European Union).

10.4 If an obligation to disclose information as stipulated in Section 10.3 above emerges, the Data Processor shall immediately inform the Data Controller of such situation if not prohibited by applicable European Union law or laws of a member state of the European Union.

11 AUDIT AND DOCUMENTATION

11.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate that the Data Processor has fulfilled its obligations in accordance with this DPA and Applicable Data Protection Legislation. At the Data Controller's request, the Data Processor shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. The Data Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Data Processor.

11.2 The Data Controller shall ensure that such independent third party and/or others retained to conduct an audit have entered into a confidentiality undertaking and is not a competitor to the Data Processor.

11.3 The Data Processor shall, at all times, be entitled to reasonable notice in the event the Data Controller wishes to exercise its right to conduct an audit. The Data Controller shall further ensure that an audit or inspection does not hinder the Data Processor's operations or the protection of other customers' information or personal data.

11.4 If an audit pursuant to this Section 11 indicates that the Data Processor has breached its obligations under this DPA or Applicable Data Protection Legislation, the Data Processor shall, without undue delay, remedy such deficiency.

12 LIABILITY

12.1 A Party undertakes to compensate for damage that it, or another party for which it is liable, has caused the other Party in connection with processing personal data, or in the event of actions in breach of the DPA. A Party's liability for compensation under this Section 12.1 shall be limited to fifteen (15) percent of the total fees paid under the SaaS Agreement during the 12 months immediately preceding the event that forms the basis for the claim for damages, provided that there is no intent or gross negligence. A Party shall not be liable, under any circumstance, for loss of profit or other indirect damage or loss, provided that there is no intent or gross negligence.

12.2 In the event of compensation for damages in connection with wrongful processing of personal data, which, through an established judgment or settlement, shall be payable to the data subject due to a breach of the provisions in this DPA, the Data Controller's instructions and/or Applicable Data Protection Legislation, Article 82 of the GDPR shall apply.

12.3 This liability claim, as set out in this Section 12 of this DPA, takes precedence over any liability claim in the SaaS Agreement with regards to processing of personal data.

12.4 The Parties' liability for compensation in accordance with this Section 12 will apply even if the DPA is terminated or otherwise cease to apply.

13 TERM

13.1 This DPA is effective when signed by both Parties and remains in effect for as long as the Data Processor and/or a Sub-processor process personal data on behalf of the Data Controller within the scope of the undertakings arising from this DPA and/or the SaaS Agreement. If the SaaS Agreement is terminated and a new contract with a similar scope and purpose to the SaaS Agreement is entered into directly between the Parties, while a new data processing agreement is not entered into, this DPA shall apply to the new agreement.

13.2 This DPA applies to and covers any changes, additions, or amendments to the SaaS Agreement unless the Parties enter into a new data processing agreement.

14 EARLY TERMINATION

14.1 The Data Processor shall immediately inform the Data Controller if the Data Processor, for whatever reason, is unable to fulfill its obligations under this DPA.

14.2 If the Data Processor is not able to remedy and fulfil its obligations under this DPA prior to thirty (30) days after having informed the Data Controller pursuant to Section 14.1, the Data Controller shall have the right to terminate the SaaS Agreement and this DPA.

14.3 For termination of this DPA pursuant to Sections 4.5, 4.6, 4.8 and/or 6.4 of this DPA, Section 12 of Appendix 1 to the SaaS Agreement shall apply.

15 MEASURES IN CONNECTION WITH THE TERMINATION

15.1 At the end of the provision of the Services relating to processing, the Data Processor shall, at the Data Controller's instructions, delete all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so, or, return all the personal data to the Data Controller and delete existing copies unless the Data Processor is required by European Union law or laws of a member state of the European Union to save a copy of the personal data. Until the data is deleted or returned, the Data Processor shall continue to ensure compliance with this DPA.

15.2 If such specific instructions have not been given at the end of the provision of the Services relating to processing, the Data Processor shall delete all personal data including copies within thirty (30) days from the end of the SaaS Agreement, unless the Data Processor is required by European Union law or laws of a member state of the European Union to save a copy of the personal data.

15.3 If personal data is returned, it shall be in a commonly used and standardized format, unless the Parties have agreed on another format.

15.4 In this context, deletion means that the personal data is deleted in accordance with the industry standard in force at any given time in order to make it impossible for the data to be recreated using technology or method known at the time of deletion. This shall also apply to personal data that has been processed for logging and security purposes.

16 AMENDMENTS

16.1 If Applicable Data Protection Legislation changes during the term of this DPA, or if competent supervisory authority issues guidelines, decisions or regulations concerning the application of Applicable Data Protection Legislation that result in this DPA no longer meeting the requirements for a data processing agreement, this DPA shall be changed in order to meet such new or additional requirements. The Parties shall mutually and in writing agree on such changes.

16.2 Other amendments and additions to the DPA shall, in order to be binding, be in writing and duly signed by both Parties. If the SaaS Agreement specifies a process for amendments to the agreement, this shall also be applicable in regard to amendments to this DPA.

17 GOVERNING LAW AND DISPUTE RESOLUTION

17.1 What is stipulated in the SaaS Agreement regarding governing law and dispute resolution also apply to this DPA.

SUB-APPENDIX 1 – INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

The following document is the Data Controller's instructions to the Data Processor.

Definitions used in this instruction shall have the same meaning as in the DPA, unless circumstances clearly indicate otherwise.

1. PROCESSING OF PERSONAL DATA

1.1. Purpose of processing.
The personal data is generated by users or collected from another system through custom made integrations. The purpose of processing this personal data is to present the information on interactive visualization boards used for sharing information, planning and follow up on status of tasks, projects, goals and similar user generated information. Personal data may also be processed to a limited extent for the purpose of receiving technical assistance in relation to the Services as well as error proofing, security monitoring, and technical development.

1.2. Subject-matter of the processing.
The subject-matter of the processing is the provision of the Data Processor's Services including related technical assistance and development.

1.3. Categories of personal data.
The Service will process information about the registered users of the Service, such as full name, telephone number, email address, photo, IP address.

Information generated by the users, such as responsibilities, tasks, schedule, goals.

The Service will log the standard data provided by the user's web browser. It may include the computer's Internet Protocol (IP) address, browser type and version, visited pages, the time and date of the visit, the time spent on each page, and other details. The Service will also collect data about the device the employee is using to access the Services. This data may include the device type, operating system, unique device identifiers, device settings, and geo-location data depending on the settings of the device. The purpose of processing this information is to use it for error proofing, security monitoring, and technical development.

1.4. Categories of data subjects.
The processing of personal data under this DPA applies to the Data Controller's employees (incl. current and former employees, trainees and interns), and the Data Controller's business partners (subcontractors incl. its employees).

1.5. Processing activities (nature of the processing).
Collection, structuring, storage, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

1.6. Transfer to third countries.
The locations/countries listed in Sub-Appendix 2 – List of approved Sub-processors or as shown in the list of the Sub-processors in accordance with Section 8.4 of the DPA.

1.7. Duration.
The Data Processor deletes personal data at the Data Controller's request (if applicable in the specific

Services). The Data Controller also has the option to delete certain data manually in the Services. After the DPA has ceased to apply: see Section 15.

2. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

2.1. The Data Processor shall maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data uploaded to the services as described in the controls of the international standard ISO 27001:2022 that are reasonably relevant for the services.

2.2. The Data Processor shall ensure that physical data center access is only provided to approved persons with a valid business justification.

2.3. The Data Processor shall take the following measures to prevent unauthorized access and use of related information technology systems:

a) be able to provide an up-to-date list of all individuals that have access to the services, including administrator rights, and;

b) log activities that are reasonably relevant for the processing of personal data in the services, and;

c) support the Data Controller in setting up access control, IP whitelisting and blacklisting, multi-factor authentication or single sign-on in the services.

2.4. The Data Processor shall take the following measures to prevent unauthorized reading, copying, modification or erasure when personal data is electronically transferred or in the context of transfer or storage on a storage medium as well as to ensure that the recipient of the personal data can be identified and controlled when personal data is transferred electronically:

a) all communication between client and server and when persistently stored in a database on the server shall be encrypted with industry standard methods, and;

b) personal data shall be backed up daily as a minimum, and;

c) personal data shall not be accessible or transferred in any other way than through the services unless otherwise agreed.

2.5. The Data Processor shall take measures to ensure that the personal data which is processed for different purposes are processed separately and that the Data Processor’s other personal data, including the personal data of other customers, is separated from the personal data belonging to the Data Controller.

2.6. The personal data shall only be erased by the Data Processor when requested to do so by the Data Controller during the term of the Agreement.

SUB-APPENDIX 2 – LIST OF APPROVED SUB-PROCESSORS

Definitions used in this list of approved Sub-processors shall have the same meaning as in the DPA, unless circumstances clearly indicate otherwise.

The Data Processor is entitled to engage the following Sub-processors for the processing of personal data within the scope of this DPA.

Name of Sub-processor and address	Description of the services/sub-processing	Location for the processing of personal data (country)	Safeguards for transferring of personal data to third country
Amazon Web Services Inc. 410 Terry Avenue North Seattle, WA 98109-5210, USA	Misc. services, e.g. files hosting and SMTP.	Ireland	Data processing agreement including European Commission's standard contractual clauses for international transfers.
MongoDB, Inc. 1633 Broadway, 38th Floor New York, NY 10019, USA	Object database hosting.	Ireland	Data processing agreement including European Commission's standard contractual clauses for international transfers.
Elasticsearch B.V. Keizersgracht 281 1016 ED Amsterdam The Netherlands	Database hosting.	Ireland	N/A
Redis Labs Inc. 700 E El Camino Real S. 250 Mountain View, CA 94040, USA	Database hosting.	Ireland	Data processing agreement including European Commission's standard contractual clauses for international transfers.
84codes AB Sveavägen 98 113 50 Stockholm, Sweden	Message broker hosting.	Ireland	N/A
Coralogix, Ltd. Menachem Begin 150, 18 Floor Tel Aviv, Israel	Centralized log hosting.	Ireland	EU adequacy decision.
OpenAI OpCo, LLC 3180 18th St., San Francisco, CA 95110, USA	Artificial intelligence model for chatbot.	USA	Data processing agreement including European Commission's standard contractual clauses for international transfers.