ELOOMI DATA PROCESSING AGREEMENT

Version 5.6 published July 5, 2023

1. BACKGROUND

1.1 The customer (data controller) and eloomi (data processor) have entered into an agreement regarding the data controllers' access to the eloomi services delivered as a software as a service application. The data controller will use the data processor's services according to the eloomi agreement (Agreement) and eloomi terms and conditions (Terms), from now on unified called the Master Agreement. This Data Processing Agreement (DPA) is enclosed as an addendum to the master agreement and does not entail any changes in the commercial terms and conditions agreed upon by the parties in the master agreement.

1.2 As part of the fulfilment of the duties under the master agreement, the data processor may process certain personal data on behalf of the data controller. The purpose of this DPA is therefore to govern the parties' rights and obligations under the Regulation (EU) 2016/679 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 (hereafter the "General Data Protection Regulation" or "GDPR"), including the framework for the data processor's processing of personal data, to ensure that the personal data processing is performed in accordance with GDPR, and not processed unlawfully or exposed to any unauthorised persons.

1.3 By agreeing to this DPA the parties acknowledge that the data processor has met sufficient guarantees for them to implement appropriate technical and organisational measures that ensures that the control of personal data always meets the applicable data processor requirements listed in GDPR, including protecting the rights of the data subjects, and the data controller also acknowledges that it complies with all data controller obligations under GDPR.

2 PURPOSE

2.1 The data processor shall according to the master agreement provide the services agreed upon as governed by the master agreement.

2.2 In order for the data processor to deliver products and services to the data controller and meet the requirements pursuant to the master agreement, the data processor will, from time to time, receive access to and process personal data on behalf of the data controller. The data processor's processing and storing of personal data shall only be performed in accordance with the Instructions and should not occur to a greater extent or last longer than what is necessary to meet the purpose for which the personal data was made available to the data processor.

3 THE DATA CONTROLLER DUTIES

3.1 At all times, the data controller must comply with its obligations under GDPR and is responsible for processing the personal data in accordance with GDPR, including that the basic principles for the handling of personal data are met. Additionally, the data controller is responsible for any actions required to meet a request from a data subject.

3.2 The data controller has performed an evaluation of the risk related to the use of the data processor, before entering this DPA and master agreement, and found it safe and in accordance with GDPR.

3.3. Considering the principles of GDPR, including the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller will only supply personal data when it is not reasonably practical to supply Redacted Materials for the data processor to comply with the Instructions.

4 THE DATA PROCESSOR DUTIES

4.1 The data processor does not have a general right of use to the personal data that is being processed according to this DPA and cannot process these for its own purposes. The data processor can only process personal data in accordance with this DPA and the instructions given by the data controller (the "Instructions"), and other written routines and instructions for processing that may be agreed in writing between the parties from time to time. Exceptions can be made if otherwise provided by law. In such case, the data processor shall inform the data controller of the legal obligation before the process begins, unless the law prohibits such notification to the data controller. The data processor shall in all cases process the personal data in accordance with the applicable processor obligations in GDPR. If the data controller unnecessarily makes personal data available to the data processor, the data processor shall promptly delete such personal data.

4.2 Processing activities may be carried out at the data processor's locations and at the sub-data processor's locations. The data controller acknowledges that the data processor and/or its sub-data processors may process customer data in countries that are outside of the EEA, United Kingdom, and Switzerland ("European Countries"). This will apply even where the data controller has agreed with the data processor to host customer data within EEA in accordance with the data processor's Regional Data Hosting Features if such non-European Countries processing is necessary to provide support or services requested by the data controller. Such transfer will rely on (a) the country ensures an adequate level of data protection (b) and/or one of the conditions listed in Article 46 GDPR (or its equivalent) is satisfied.

4.3 The data processor is obliged to give the data controller access to its security policy documentation and other relevant security documents upon the data controller's request. The data processor shall provide such assistance within the data processor's obligations pursuant to GDPR as requested in writing by the data controller from time to time as the data controller reasonably considers is necessary to comply with the data controller's own obligations under GDPR.

4.4 The data processor shall assist the data controller in fulfilling the data controller's duty to respond to requests that the data subject provides in order to exercise his rights in accordance with GDPR. Such assistance must first be agreed in writing between the parties, which may incur additional fees. If the Data Subject makes his/her rights applicable by contacting the data processor directly, the data processor shall promptly inform the data controller. The data processors are obliged to delete and/or destroy after returning all personal information provided for the data processor if the data subject has submitted such a request to the data controller.

4.5 The data processor shall hold confidential all documentation and personal data that he or she may process under this DPA. This also applies after termination of the master agreement. Access to personal data shall be limited to those of the data processor's employees who need access to the personal data to perform their duties and the implementation of the data processor's obligations under this DPA, and in accordance with the instructions. The data processor shall ensure that persons authorized to process personal data have undertaken to treat the information as confidential or are subject to an appropriate duty of confidentiality.

4.6 The data processor shall provide the data controller with the contact details of the data processor's data protection advisor, if the data processor has designated this.

4.7 The data processor is obliged to keep itself updated with regards to any changes to GDPR that may affect this DPA, and both parties to this DPA are obligated to notify the other party if they reasonably believe that this DPA is required to be varied due to such changes to the law.

4.8 In the event that the data processor becomes aware that in following the data controller's instructions it shall be breaching the terms of this DPA or GDPR, the data processor will agree with the data controller in good faith on how to vary the Instructions if necessary.

5 SUBCONTRACTORS

5.1 The data controller hereby confirms its general written authorisation for the data processor's use of sub-data processors listed at: https://eloomi.com/legal/subprocessors/. The data processor shall update the sub-data processer list on its Website of any change to sub-data processor to be appointed at least thirty (30) days prior to such change. The data controller is responsible to frequently review the Website to ensure notification. The data controller can object to any change in accordance with the procedure stated at the Website.

5.2 The data processor is responsible for own use of subcontractors, and that such use is in accordance with GDPR, including an obligation to secure that a similar data processing agreement has been entered. The data processor shall ensure that the subcontractors are familiar with the data processor's contractual and legal obligations, and the subcontractors are required to fulfil the terms thereof in the same way as the data processor.

5.3 The data processor is fully responsible for the subcontractor fulfilling its obligations to the data controller. The data processor shall remain liable to the data controller for the performance of the data processor's subcontractor's obligations.

5.4 The data processor is required to provide the data controller with a copy of the data processing agreement between the data processor and the subcontractor upon request.

5.5 The data controller can through the eloomi services gain access to link and play content and data in the solution from other third-party solutions. In such case the data controller decides to make use of this and do so, the data processer cannot be the responsible data processor. (Examples, but not limited to e.g., link to a document in a third-party solution, link to a YouTube video hosted on a third-party solution and similar).

6 SECURITY AND EXCEPTION HANDLING

6.1 Considering the nature of the processing, the data processor shall comply with the requirements for security measures provided for in GDPR that are applicable to the data processor at any time. This means, inter alia, that appropriate technical and organisational measures are taken to ensure an appropriate level of security of personal data that may be processed by the data processor in accordance with the instructions. A description of the technical and organisational measures implemented by the data processor is described in detail in Appendix C to this DPA.

6.2 The data processor shall carry out regular internal controls for the purpose of giving the data controller a sufficient guarantee that the data processor is continuously making the necessary steps, as mentioned above, to ensure appropriate information security, considering the nature of the processing, in compliance with the data processor's obligations under GDPR. In this regard, the data processor shall document the procedures and other measures to ensure that the requirements for the information security is met. Such documentation shall be made available upon written request from the data controller.

6.3 The data processor is obliged to notify the data controller in writing of any personal data breach (as defined in GDPR) of security regarding personal data security without undue delay after having become aware of the breach.

6.4 The data controller is responsible for sending a discrepancy report to the relevant data protection authority. The data processor is obliged to assist the data controller with information to ensure that the notification requirements for the data inspectorate are met. If the data controller requests, the parties will agree in writing on any additional services that the data processor may provide with respect to notifying the affected data subjects.

6.5 In connection with the data processor's processing of the data controller's personal data, the data processor may be jointly liable with the data controller for the financial loss suffered by the data subject because of a direct breach of GDPR, where such liability is imposed on the data processor under GDPR by a regulatory body authorised to do so, or by a third-party. For all other matters, the data processor's liability for all claims for a breach of any term of this DPA is as set out in the master agreement ref. clause 6 in the terms.

7 SECURITY AUDIT

7.1 From time to time, the data controller can agree with the data processor to a security audit of information systems and the like to confirm compliance with this DPA. This audit can be an acceptance of the external audit done by a third-party for eloomi's compliance audit. Each party shall bear its own costs in connection with such audit.

7.2 The data processor shall cooperate with the data controller's implementation of security audits, by making available to the data controller the necessary documentation as reasonably required, and physical premises for inspection, during normal business hours at data processor.

7.3 The data controller may use an external auditor for the implementation of a security audit, provided that such external auditor has signed a confidentiality agreement and NDA acceptable to data processor. Audits can be carried out annually by agreement.

7.4 Nothing in this section 7 will apply to audits conducted by an authority or body who may perform such audit under GDPR, where in accordance with GDPR the data processor must bear its own costs, and perform such obligations as reasonably requested.

8 DURATION

8.1 This DPA applies as long as the data processor processes personal data on behalf of the data controller.

8.2 In case of data processor's violation of this DPA, or GDPR, the data controller may instruct the data processor to stop the further processing of the personal data with immediate effect, and the parties will in good faith agree on how to rectify the violation.

9 TERMINATION

9.1 Upon termination of this DPA, the data processor is obliged to delete or return at request all personal data received on behalf of the data controller, as agreed in writing with the data controller. If personal data is to be returned on request by the data controller, and to the extent that the data processor possess such items, the following is agreed to be possible to return and shall be returned upon termination of this DPA: Copy of all personal data in databases and data files in recognised readable formats that is in data processor's possession. Reasonable costs related to return are covered by the data processor. The exception is a material breach of this DPA caused solely by the data processor, where such breach results in a termination of this DPA.

9.2 If deleting personal data, the data processor shall delete and/or properly destroy all personal data as well as copies of such that it may possess. The data processor shall on request document in writing and verify that deletion and/or destruction has happened in accordance with this DPA within a reasonable time after the termination of this DPA, and at the latest within 3 months after the termination of this DPA.

10 COMMUNICATION

10.1 Each of the parties shall name persons or responsible unit responsible for giving instructions on behalf of the data controller and receive instructions on behalf of the data processor. In relation to this DPA, the parties agree that the name stated in this DPA shall give and receive instructions relating to the processing of personal data. Each of the parties shall in writing inform the other part if the named responsible changes or is temporarily prevented from giving and/or receiving Instructions and appoint a substitute.

10.2 The data processor shall promptly inform the data controller if the data processor thinks that any instructions are in breach of the law, and certain processing may accordingly be suspended, or varied in accordance with section 4 of this DPA.

11 LAW AND VENUE

11.1 The DPA is subject to Danish law and the parties agree on Copenhagen City court as legal venue. This also applies after termination. The legal basis for processing is as described in the applicable instructions.

A APPENDIX A – DATA PROCESSING INSTRUCTIONS

A.1 These data processing instructions constitute the data controller's instructions to the data processor in connection with the data processor's processing of certain personal data in the performance of certain services under the master agreement and shall be performed in accordance with the terms of the DPA.

A.2 Data Subjects

The data controller's employees (managers of the eloomi services delivered as a software as a service application);

The data controller's end-customers (users of the eloomi services delivered as a software as a service application)

A.3 Categories of Personal Data

From time to time, the data controller may make available to data processor, for the purposes of data processor's provision of the applicable services under the master agreement, such data that includes the data subject's:

The data controller's employees: name, address, IP-address, Job title, Job-ID, Course material, Course results, Appraisals, contact details (telephone number, email address, etc.), and/or

The data controller's end-customers: name, address, IP-address, Job title, Job-ID, Course material, Course results, Appraisals, contact details (telephone number, email address, etc.)

A.4 Special categories of data

N/A

A.5 The nature of the processing and purposes of processing

Data processor may process personal data only for the purposes of providing the applicable services under the master agreement.

A.6 Lawful basis of the Processing

The lawful basis for the processing of the personal data is the following: processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.

A.7 Location of the Processing

It is agreed that the processing shall be performed at the following locations: Hosting Partner: Microsoft Azure (Ireland (EU) or USA (non-European Countries) as specified in the Order Form)

A.8 Sub-Data Processors

The data controller authorises the sub-data processors as specified in Appendix B.

A.9 Standard Contractual Clauses

Where eloomi processes personal data in non-EEA countries, eloomi will in some cases rely on the EU Commission' Standard Contractual Clauses (annexed to EU Commission Decision 2021/914/EU of 4 June 2021) (the "EU SCCs") which, if the recipient country does not ensure an adequacy decision, shall be entered into and incorporated into this DPA by this reference and completed as follows:

(i) Module 2 (Controller to Processor) will apply where the customer is a data controller of personal data and eloomi is a processor of the personal data; Module 3 (Processor to Processor) will apply where the customer is a processor of the personal data and eloomi is a processor of the personal data. For each Module, where applicable:

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub data processor changes shall be as set out in this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 12, any claims brought under the EU SCCs shall be subject to the eloomi terms and conditions. In no event shall any party limit its liability with respect to any data subjects rights under the EU SCCs.

(vi) in Clause 17, Option 1 will apply, will be governed by Danish Law;

(vii) in Clause 18(b), disputes shall be resolved before the courts of Copenhagen, Denmark;

(viii) Annex I of the EU SCCs shall be deemed completed with the information set out in the Appendix A to this DPA; and

(ix) Annex II of the EU SCCs shall be deemed completed with the information set out in Appendix C to this DPA.

(x) To the extent any export from or processing of personal data outside the United Kingdom is subject to applicable data protection law in the United Kingdom (including UK GDPR and Data Protection Act 2018) ("UK Data Protection Laws"), for so long at the Parties is permitted to rely on the EU SCCs for transfers of personal data from the UK subject to completion of a UK Addendum to the EU SCCs issues by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("UK Addendum"), then the EU SCCs, completed as set out above in Clause A.9(i)-(ix) of this DPA shall also apply to transfers of such Personal Data, subject to the provision that the UK Addendum shall be deemed executed between eloomi and the customer, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such personal data.

B APPENDIX B – SUB-CONTRACTORS

B.1 https://eloomi.com/legal/subprocessors/

C APPENDIX C – SECURITY MEASURES BY THE DATA PROCESSOR

C.1 IT security policy.

It is important for eloomi that eloomi employees know what is expected and required of them when using systems as well as in general - internet and email use, security, software, hardware storage and data storage.

C.2 Compliance

eloomi has defined a set of information security policies that are approved by management and communicated to employees. The information security policies are reviewed at scheduled intervals or if significant changes occur. Every employee at eloomi must adhere to the "eloomi IT security policy" and bound by the confidentiality of the employee contract. The compliance course must be renewed once a year.

C.3 IT risk analysis

Once a year, eloomi's security team analyses IT risks that may affect operations, customer data or information security. Risks are evaluated on two axes; Probability and impact. The result of the analysis is risks that may occur and affect eloomi's operations as a SaaS supplier as well as the customer's security for safe storage. The probability of this happening is measured in a range from very likely to very unlikely - and necessary measures and implementations are made on the basis of the analysis.

C.4 GDPR

eloomi stores information about customers and business contacts in accordance with the Personal Data Act. All the system with personal data is continuously registered in a data processor log, where type, owners, expiration, security measure and responsibilities are defined. In addition, all eloomi employees must pass a compliance course each year in eloomi's IT security policy as well as a compliance test on the management of sensitive data. The results of a test are saved and are part of a control in our annual IT audit.

C.5 General safety precautions

eloomi has formalized procedures for information security based on regulatory requirements, standards, and good data processing practices. The purpose is to ensure the continued confidentiality, integrity, availability and robustness of processing systems and services, to ensure that personal data are not lost or fall into the wrong hands, and to prevent the harmful effects that such breaches may have on data subjects. eloomi also has procedures, in accordance with applicable standards, for regular testing, assessment and evaluation of the technical and organizational measures.

C.6 Test environment

In rare cases, personal data is processed in a test environment, and when used, the requirements for the security level are the same as described in this instruction. Test environments are physically separated from production environments.

C.7 Instruction of employees etc.

eloomi has ensured that employees and any business partners are constantly familiar with and have adequate training and instruction on the purposes of data processing, policies, procedures, and their duty of confidentiality.

C.8 Network and encryption

The data processor has appropriate technical measures to protect systems and networks, including protecting data during transmission and access via the Internet, as well as to limit the risk of unauthorized access and / or installation of malicious code.

C.9 Access management and administration of user access

Only employees who have a work-related need to process personal data in relation to the Agreement have access to personal data. And only those persons who are authorized to do so by the authorized person may have access to the personal data. A list of authorized employees is kept, indicating the type of access the authorization covers. The list of authorized employees is continuously updated in accordance with good data processing practice. At the end of the service, the employees' access is closed. In addition, eloomi uses secure identification and authorization technologies, including secure passwords. The authentication mechanisms used live up to the latest guidance from the Danish Digitization Agency, and good practice in the area.

C.10 Contingency plan

eloomi has a documented contingency plan that ensures the re-establishment of services without undue delay in the event of operational interruptions under the main agreement.

C.11 Backup

Backup of configuration files and data must take place daily in an uninterrupted process so that relevant data can be re-established at least 7 days back. The backup copies are stored in such a way that they are not accidentally or illegally (eg by fire, flood, accident, theft or the like) destroyed, lost, degraded, come to the knowledge of unauthorized persons, misused or otherwise treated in violation of the rules in force at any time and regulations for the processing of personal data. The backups are stored physically separate from primary data in our data centre at Microsoft Azure, Ireland. It is tested every month that data can be restored from backups.

C.12 Change management

eloomi has formal change management procedures in place to ensure that any changes are properly authorized, tested, and approved prior to implementation. The procedure is supported by effective functional separation and/or management follow-up to ensure that no individual can control a change alone.

C.13 Physical protection and environmental protection

eloomi has physical security measures for the security of premises used for the processing of personal data, including the storage of personal data covered by the Data Processor Agreement against unauthorized access and tampering.

C.14 Disposal of equipment

eloomi has formal processes in place to ensure the effective erasure of personal data prior to the disposal of electronic equipment.

C.15 Clean desk policy

eloomi's Clean Desk Policy specifies how eloomi employees should leave their workspace when leaving the office. Confidential data and access to these is therefore limited. This also includes possible access to data from our cleaning staff and other external visitors to eloomi offices.

C.16 Logging

Logging has been established on the administrators' actions in the system, and log files are stored separately with additional access security.

D APPENDIX D – NAMED CONTACTS

Data processor is eloomi A/S, company number 36699752, Per Henrik Lings Alle 4, 2100 Copenhagen, Denmark. Named contact is the Data Protection Responsible Unit at private@eloomi.com. Data controller is unless otherwise informed by the data controller, contact data from the master agreement.