ELOOMI EU DATA PROCESSING AGREEMENT

Version 2.0 published 02 February 2021

Data processor: eloomi A/S, Company number 36699752, Per Henrik Lings Allé 4, 2100 Copenhagen, Denmark.
Contact: Kenneth Granno at kenneth@eloomi.com.

Data controller:

Contact:

Date:

Master Agreement:
This agreement including Appendix A, B & C is made in 2 - two copies, whereof the parties have one each.

Data processor, eloomi A/S	Data controller,

1. The Data Processing Agreement background and purpose

The parties have entered into an Agreement regarding a cloud service enabling the Data Controller to use eloomi's product and services according to the Master Agreement and Terms and Conditions, from now on called the Master Agreement. This Data Processing Agreement, from now called 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. The parties have incorporated a reference to this Agreement in the Master Agreement terms clause 5.

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.

By signing this DPA the parties acknowledge that the data processor has met sufficient guarantees in order for them to implement appropriate technical and organisational measures that ensures that the control of personal data meets the at all times 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.

This Agreement will replace any previous Data Processing Agreements that have been entered into.

2. The purpose of the processing of data

The data processor shall according to the Master Agreement provide the products and services agreed upon as governed by the Master Agreement.

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 in order to meet the purpose for which the personal data was made available to the data processor.

3. The data controller's duties

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 is met. Additionally, the data controller is responsible for any actions required to meet a request from a data subject.

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

Taking into account 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 in order for the data processor to comply with the Instructions.

4. The data processor's duties

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.

Before transferring personal data to any location not listed in the Instructions, the parties shall agree in writing to vary the Instructions to include that location. If such transfer is outside of the European Economic Area, the data processor is obliged to ensure that the transfer has a legal transfer basis.

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 in order to comply with the data controller's own obligations under GDPR.

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.

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 in order 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.

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.

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.

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. Use of subcontractor

If the data processor makes use of a subcontractor, such use of subcontractor has to be agreed upon in writing with the data controller before processing the personal data. An overview of approved subcontractors is attached as Appendix B. The attachment shall be updated if changes are made in use of subcontractors.

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 into. 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.

If the data processor uses subcontractors that involve the transfer of personal data to third countries, the data processor is obliged to ensure that the transfer has a legal transfer basis and otherwise complies with GDPR.

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.

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.

The data processor does in eloomi give the possibility for the data controller to link and play content and data in the solution. In such case the data controller decides to make use of this, the data processer cannot be the responsible data processor.

6. Security and exception handling

Taking into account 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 organizational 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 organizational measures implemented by the data processor is described in detail in Appendix C to this Agreement.

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, in order to ensure appropriate information security, taking into account 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 in order to ensure that the requirements for the information security is met. Such documentation shall be made available upon written request from the data controller.

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.

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.

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 as a result of a direct breach of GDPR, where such liability is imposed on the data processor under GDPR by a regulatory body authorized to do so, or by a third party. For all other matters, each party's liability to the other for all claims for a breach of any term of this DPA is as set out in the Master Agreement.

7. Security Audit

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

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.

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.

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 of the DPA

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

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. Upon termination

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, 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 recognized readable formats that is in data processor's possession. Costs related to return are covered by the data controller. 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.

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 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/Information

Each of the parties shall name persons 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 persons 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 person responsible changes or is temporarily prevented from giving and/or receiving Instructions and appoint a substitute.

The data processor shall promptly inform the data controller in the event that 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. Legal basis and venue

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

APPENDIX A – Data Processing Instructions Template

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. The details of the Data Processing Instructions are set out below:

1. Data Subjects

The Data Subjects are:

The Data Controller's employees (managers of cloud solution);

The Data Controller's end-customers (users of cloud solution)

2. 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, contact details (telephone number, email address, etc.)

The Data Controller's end-customers: name, contact details (telephone number, email address, etc.)

Etc.

3. Special categories of data

N/A

4. 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.

5. 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 in order to take steps at the request of the data subject prior to entering into a contract.

6. Location of the Processing

It is agreed that the Processing shall be performed at the following locations: Hosting Partner: Microsoft Azure (Within EU)

https://azure.microsoft.com/en-us/global-infrastructure/regions/

7. Sub-Data Processors

The Data Controller authorizes the sub-Data Processors as specified in appendix B.

APPENDIX B - Specification of sub-contractor

According to the data processing agreement clause 5 between the parties, the data processor can use specific sub-contractors after prior written approval from the data controller. This Appendix B contains a detailed description of which sub-contractors the data processor can use.

Microsoft Azure : Data hosting : Within EU

TwentyThree : Video Streaming : Within EU

APPENDIX C – Description of security measures implemented by the data processor

1. Secure infrastructure & process

The eloomi infrastructure has been certified and is being audited to meet the most stringent requirements globally:

• ISAE 3402 Type II Microsoft Azure hosting

• ISAE 3000 eloomi Change Management and IT Policy

Every employee in eloomi knows the IT Policy, get frequent training and has confidentiality clauses in their employment contracts.

2. Password & SSO security

To keep the user access safe, eloomi enforces 2 factor authentications, where possible and requires strong passwords that match industry standards and requirements. Unsuccessful attempts to login will result in the user account being suspended for a specific time. If the login attempts continue to fail for a specific number of attempts the account will be suspended. Reactivation of the account then requires a manual administration procedure. In addition, user sessions, which are authenticated, expire when the user has been inactive for a specific number of minutes.

Customers may use Single Sign On (SSO) which requires users to be authenticated via an identity provider. Other authentication tools or social login possibilities like Facebook, LinkedIn & Google can be used as well.

3. Personal Data

eloomi handles personal data that is covered by the GDPR requirements. This data includes e.g. name, email, ID number and other unique identifiers.

No employees have access to confidential or personal data in applications and systems unless they are authorized personnel whose tasks and responsibilities require access.

Access permission including all temporary and durable access to IT tasks and job roles is the responsibility of and requires eloomi´s IT management approval.

Mandatory criteria for managing access rights and control via Access Control Lists comprise:

• Overview of user roles and access profile

• Process for adding, changing and revoking access rights

The access control is documented for all applications, it systems and environments giving access to sensitive information or personal data.

4. The right to be forgotten

Users can be confident that their personal data has been backed up in accordance with GDPR principles of privacy by design and the right to be forgotten.

The right to be forgotten is a main pillar in GDPR. This principle, which makes it possible to identify the location of personal data – either all company data or individual user data – and to delete or anonymize it, is incorporated in all systems and processes. It is possible to choose how long it will take before deleted users are anonymized. By default, deleted users are automatically anonymised after 72 months.

5. Audit logging

Another major change imposed by the GDPR is the audit logging. To make sure eloomi and our customers are compliant with the regulation our systems are logging who (users, admins, operators) are e.g. Viewing and editing which data and when. Unsuccessful user login attempts are also logged.

Audit logs are stored for 5 years in a safe place with restricted access.