Annex C. Data Processing Agreement

Microbizz by Ventu A/S
Lindgreens Allé 12, 1. tv.
DK-2300 Copenhagen S
Denmark
VAT DK34469741

+45 7023 5323

info@microbizz.com

Scan the QR code and visit microbizz.com

ANNEXES TO THE DATA PROCESSING AGREEMENT

Change log

Version	Date	Updated by	Change
2.0	05-09-2019	Dan Aggerholm, COO	Updated in relation to GDPR
2.1	06-12-2019	Dan Aggerholm, COO	Annex 1: Updated
2.2	02-06-2021	Michael Sahl, CTO	Annex 4: DigitalIQ added as sub-data processor
2.3	22-09-2022	Troels Ladefoged, Process specialist	Item 5.4 added Annex 4: Addresses added for sub-data processors
2.4	01-06-2023	Troels Ladefoged, Proces specialist	Signature of Camilla Simonsen in her capacity as new CEO
2.5	04-09-2023	Troels Ladefoged, Proces specialist	Annex 4: TrueCommerce replaces ID Solutions. Delivers the same services. Name change for Linode to Akamai due to acquisition
2.6	12-10-2023	Troels Ladefoged, Proces specialist	The data processing agreement is incorporated as an integrated appendix to the cooperation agreement and is thus not signed separately. The list of sub-processors in Annex 4 has been moved to a page in the Micropedia website. Annex 4 includes a link to this webpage.

1 BACKGROUND AND PURPOSE

1.1 The Parties have agreed on the provision of certain services by the Data Processor to the Data Controller, as further described in the Parties' separate agreement thereto and Annex 1 to this Agreement ("Main Services").

1.2 In this context, the Data Processor processes personal data on behalf of the Data Controller and the Parties have therefore concluded this agreement and its annexes ("Data Processing Agreement").

1.3 The purpose of the Data Processing Agreement is to ensure that the Data Processor complies with the personal data law regulation applicable from time to time, including in particular:

a) GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)
b) Data Protection Act, Law No 502 of 23 May 2018

2 SCOPE

2.1 The Data Processor is authorised to carry out the processing of personal data on behalf of the Data Controller under the conditions set out in the Data Processing Agreement.

2.2 The Data Processor may process personal data only upon documented instructions from the Data Controller ("Instruction"). This Data Processing Agreement including its annexes constitutes the Instruction at the time of signature.

2.3 The Data Controller shall determine the duration and nature of the processing, the purposes for which the personal data are processed and the data processing practices that may be used. Thus, the processor may not process the personal data for its own purposes or use more intrusive measures than are justified by the purpose.

2.4 If the Data Processor considers that an instruction is contrary to the laws, regulations, and practices in force at any time in the EU and the Member States relating to the processing of personal data, including the Data Protection Regulation and the Data Protection Act (Act No 502 of 23/05/2018), the Data Processor must notify the Data Controller immediately and before any processing is carried out.

3 OBLIGATIONS OF THE DATA PROCESSOR

3.1 Technical and organisational security measures

3.1.1 The processor is responsible for implementing the necessary (a) technical and (b) organisational measures to ensure an adequate level of security. The measures shall be implemented taking into account the current state of the art, and the nature, scope, composition and purposes of the processing in question, as well as the risks of varying probability and severity to the rights and freedoms of natural persons. The data processor shall take into account, inter alia, the category of personal data described in Annex 1 when determining these measures.

3.1.2 Notwithstanding Clause 4.1, the Data Processor shall implement the technical and organisational security measures set out in (a) Annex 2 to this Data Processing Agreement and (b) the agreement(s) for the provision of the main services.

3.1.3 The Data Processor shall implement the appropriate technical and organisational measures in such a way that the Data Processor's processing of personal data complies with the requirements of the personal data protection regulations applicable at any given time.

3.1.4 The Parties agree that the guarantees set out in Annex 2 are adequate at the time of the conclusion of this Data Processing Agreement.

3.2 Employee relations

3.2.1 The Data Processor shall ensure that employees processing personal data for the Data Processor are bound by confidentiality obligations or are subject to an appropriate legal obligation of confidentiality.

3.2.2 The Data Processor and its employees shall be prohibited from obtaining information of any kind whatsoever which is not relevant to the performance of their tasks.

3.3 Evidence of compliance with obligations

3.3.1 The Data Processor shall, upon written request, provide evidence to the Data Controller that the Data Processor:

a) Complies with its obligations under this Data Processing Agreement and the Instructions.
b) Complies with the provisions of the personal data protection legislation in force at any time in respect of the personal data processed on behalf of the Data Controller.

3.3.2 The Data Processor shall document this without undue delay.

3.3.3 The Data Controller, a representative of the Data Controller or its auditors (both internal and external) shall have access to carry out inspections and audits at the Data Processor, to obtain documentation, including logs, to ask

questions, etc., in order to ascertain the Data Processor's compliance with the requirements arising from this Data Processing Agreement.

3.3.4 In the event that the Data Controller and/or relevant public authorities, in particular the Danish Data Protection Agency, wish to carry out an inspection of the above measures pursuant to this Agreement, the Data Processor and its sub-data processors undertake to make time and resources available for this purpose.

3.3.5 The Data Processor shall review at least once a year its internal security rules and guidelines for the processing of personal data in order to ensure that the necessary security measures are constantly observed, in accordance with this Clause 3 and Annex 1. See Annex 3 for the detailed content of the Data Processor's obligations.

3.4 Security breaches

3.4.1 The Data Processor shall notify the Data Controller of any personal data breach that could potentially lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data processed for the Data Controller ("Security Breach").

3.4.2 Security Breaches must be notified to the Data Controller immediately - and no later than 24 hours - after the Data Processor becomes aware of the Breach, so as to allow the Data Controller to comply with any obligation to notify the Danish Data Protection Agency of the Breach within 72 hours.

3.4.3 Data Processors shall not communicate publicly or to third parties about personal data breaches without the prior written consent of the Data Controller.

3.5 Assistance

3.5.1 The Data Processor shall, taking into account the nature of the processing, assist the Data Controller in the performance of its obligations in processing the Personal Data covered by this Data Processing Agreement, including by:

a) the obligation to implement appropriate technical and organisational security measures.
b) Responses to data subjects when exercising their rights.
c) the obligation to notify security breaches and to inform the data subject of breaches.
d) the obligation to conduct impact assessments.
e) the obligation to consult the Danish Data Protection Agency.

3.5.2 The processor shall be entitled to payment for time spent and materials used for assistance provided pursuant to this Section 3.5 and Section 3.3.4 unless otherwise provided in the agreement.

4 THE OBLIGATION OF THE CONTROLLER

4.1 The Data Controller is responsible for the personal data that the Data Controller instructs Data Processors to process. The Data Controller is responsible for ensuring that the personal data that the Data Controller instructs the Data Processor to process may be processed by the Data Processor, including that the processing is necessary and legitimate for the performance of the Data Controller's tasks.

4.2 The Data Controller shall have the rights and obligations conferred on a Data Controller by law, as set out in Clause 1.3 of the Data Processing Agreement.

5 SUB-DATA PROCESSORS

5.1 The Data Processor may only use a third party for the processing of personal data for the Data Controller ("Sub-data processor") to the extent set out in Annex 4 to this Data Processing Agreement, or as instructed by the Data Controller.

5.2 Thus, the Data Processor shall also obtain the Data Controller's written approval in the event that the Data Processor undertakes the replacement of existing Sub-data processors. The Data Controller may object to a change only if there are compelling reasons and the Data Controller can demonstrate that a new sub-data processor does not meet the applicable security requirements.

5.3 The Data Processor and the Sub-data processor shall enter into a written agreement imposing on the Sub-data processor the same data protection obligations as are imposed on the Data Processor (including by this Data Processing Agreement). The Data Controller may at any time require the Data Processor to provide evidence of the existence and content of sub-data processing agreements for the sub-data processors used by the Data Processor in the performance of its obligations to the Data Controller.

5.4 The Data Processor undertakes to include in agreements with the Sub-data processor the Data Controller as a third party beneficiary in the event of the bankruptcy of the Data Processor, so that the Data Controller can subrogate to the rights of the Data Processor and enforce them against Sub-data processors, for example, to enable the Data Controller to instruct Sub-data processors to delete or return the personal data.

5.5 The Data Processor shall be directly responsible for the Sub-data processor's processing of personal data in the same way as if the processing had been carried out by the Data Processor itself.

6 TRANSFERS TO THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

6.1 The Data Processor shall not transfer personal data to third countries or international organisations.

7 DATA PROCESSING OUTSIDE THE SCOPE OF THE INSTRUCTIONS

7.1 The Data Processor may process personal data outside the Instructions in cases where it is required by EU law or national law to which the Data Processor is subject.

7.2 In the event of processing of personal data outside the Instructions, the Data Processor shall inform the Data Controller of the reason. The notification must be made before the processing is carried out and must include a reference to the legal requirements underlying the processing.

7.3 Notification shall not be made if notification would be contrary to EU or national law.

8 AMENDMENT OF THE INSTRUCTIONS

8.1 Prior to any amendments to the Instructions, the Parties shall, to the extent possible, discuss and, if possible, agree on the implementation of the amendments, including the implementation time and costs.

8.2 To the extent not otherwise agreed, the following shall apply:

a) The Data Processor shall be entitled to payment of all costs directly related to changes to the Instruction, including implementation costs and increased costs for the provision of the Core Services
b) The Data Processor shall be obliged to comply with any changes to the extent that these are necessary to comply with applicable legal requirements

9 LIABILITY AND LIMITATIONS OF LIABILITY

9.1 The limitation of liability in the Cooperation Agreement (Section 7) shall also apply to liability arising from a breach of the Data Processing Agreement. However, the limitation of liability shall not apply to any claims of third parties (data subjects) against the Data Controller, as data controller, for losses resulting from the failure of the Data Processor to comply with the Data Processing Agreement concluded.

9.2 The Parties disclaim any liability for indirect losses, including operational losses, increased operational costs, lost savings or lost profits. It is specified that any claim by a third party (the data subjects) against the Data Controller as data controller, for losses resulting from the failure of the Data Processor to comply with the concluded data processing agreement, shall be counted as a direct loss.

9.3 The liability of the Parties for all cumulative claims under this Data Processing Agreement shall be limited to the limitation of liability set forth in the Agreement.

10 FORCE MAJEURE

10.1 The regulation of force majeure in the agreement(s) for the provision of the Main Services shall also apply to this Data Processing Agreement as if this Data Processing Agreement were an integral part thereof. In the event that the agreement(s) for the provision of the Principal Services does not address this, the provisions of this clause shall apply to this Data Processing Agreement.

10.2 The Data Processor shall not be liable for circumstances that can generally be described as force majeure, including, but not limited to, war, riots, terrorism, riots, strikes, fires, natural disasters, currency restrictions, import or export restrictions, interruption of normal traffic, interruption or failure of energy supply, public data facilities and communication systems, prolonged illness of key employees, viruses and the occurrence of force majeure at the Sub-data processor.

11 CONFIDENTIALITY

11.1 The confidentiality provisions of the agreement(s) for the provision of the Core Services shall also apply to this Data Processing Agreement as if this Data Processing Agreement were an integral part thereof. In the event that the agreement(s) for the provision of the Principal Services does not address this issue, the provisions of this Section 11 shall apply to this Data Processing Agreement.

11.2 Information relating to the content of this Data Processing Agreement, the underlying Core Services, the business of the other Party, which is either identified as confidential information in the context of the transfer to the receiving Party, or which by its nature or otherwise must clearly be perceived as confidential, shall be treated confidentially and with at least the same care and discretion as the Party's own confidential information. Data, including personal data, shall always constitute confidential information.

12 TERMINATION

12.1 Termination and Cancellation. The Data Processing Agreement may only be terminated or cancelled in accordance with the provisions on termination and cancellation in the agreement(s) for the provision of the Core Services and the terms of the Data Processing Agreement.

12.2 Notwithstanding the termination of the Data Processing Agreement as set out in clause 10.2, the Data Processor and any Sub-data processor shall remain obliged to process personal data in accordance with the Data Processing Agreement for as long as the Data Processor and any sub-data processors process the personal data on behalf of the Data Controller.

12.3 The Data Processor and its Sub-data processors shall return all personal data processed by the Data Processor under this Data Processing Agreement to the Data Controller upon termination of the Data Processing Agreement, to the extent that the Data Controller is not already in possession of the personal data. The Data Processor shall then be obliged to delete all personal data of the Data Controller. The Data Controller may request the necessary documentation that this has been done.

12.4 Notwithstanding the termination of the Data Processing Agreement, Clause 11 of the Agreement regarding confidentiality and Clause 13 regarding dispute resolution shall continue to have effect after the termination of the Data Processing Agreement.

12.5 The Data Processing Agreement previously concluded shall be terminated.

13 DISPUTE RESOLUTION

13.1 The dispute resolution rules, including the law applicable and the place of jurisdiction, in the agreement(s) for the provision of the Core Services shall also apply to this Data Processing Agreement as if this Data Processing Agreement were an integral part thereof.

ANNEX 1 - MAIN SERVICES (INSTRUCTIONS)

14 MAIN SERVICE (INSTRUCTIONS)

14.1 The Data Controller hereby instructs the Data Processor to carry out the processing of the Data Controller's data for the purpose of operating Microbizz, in accordance with the Main Agreement (as of 21/12/2015).

14.2 If the Data Processor entrusts the processing of the Data Controller's data to Sub-data processor, the Data Processor is responsible for entering into written (sub)processing agreements with them, in accordance with point 5 of the Agreement. The Data Processor shall be responsible for ensuring that any Sub-data processor comply with this instruction.

14.3 Purpose and description of the processing

14.3.1 The processing of the Data Controller's data is carried out in accordance with the purpose of the Main Agreement.

14.3.2 The Data Processor shall not use the data for any other purpose.

14.3.3 The data shall not be processed on the instructions of anyone other than the Data Controller.

14.3.4 Third countries (non-EU member states)

14.3.4.1 The Data Processor shall not transfer personal data to any third country.

14.3.5 Type of personal data

14.3.5.1 The processing operations contain personal data in the categories ticked below. The level of security of processing by the processor and any Sub-data processor should reflect the sensitivity of the data, as set out in Annex 1.

14.3.5.2 General personal data (as referred to in Article 6 of the Data Protection Regulation), including names, addresses, telephone numbers, e-mail addresses, etc.

14.3.5.3 Sensitive personal data (see Article 9 of the Data Protection Regulation):

- ☐ Racial or ethnic origin
- ☐ Political opinion
- ☐ Religious beliefs
- ☐ Philosophical beliefs
- ☐ Trade union membership
- ☐ Genetic data
- ☐ Biometric data
- ☐ Health data, including abuse of medicines, drugs, alcohol, etc.
- ☐ Sexual relationship or sexual orientation of a natural person

14.3.5.4 Personal data relating to criminal convictions and offences (see Article 10 of the Data Protection Regulation):

- ☐ Criminal convictions
- ☐ Criminal offences

14.3.5.5 Data on social security number (see Article 11 of the Data Protection Act)

- ☐ Social security numbers

14.3.6 Third countries (non-EU countries)

14.3.6.1 The data processor shall not transfer personal data to any third country.

.

ANNEX 2 - TECHNICAL AND ORGANISATIONAL SECURITY REQUIREMENTS AND GUARANTEES

15 SPECIFIC TECHNICAL AND ORGANISATIONAL SECURITY REQUIREMENTS

15.1 Introduction

This Annex describes the technical and organisational security measures that the Data Processor is responsible for implementing, maintaining, and ensuring compliance with at its Sub-data processor under the Agreement.

15.2 ISO27002

The Data Processor has implemented an internal security policy based on the principles of ISO-27002 and covering the following topics:

a) Risk assessment and management
b) Information security policies
c) Organisation of information security
d) Personnel security
e) Asset management
f) Access control
g) Physical and environmental security
h) Operational security
i) Communication security
j) Acquisition, development, and maintenance of systems
k) Supplier relationships
l) Information security breach management
m) Information security aspects of emergency, contingency and recovery management
n) Compliance

15.3 The Data Processor shall review its overall internal security policy at least annually to ensure that it complies with applicable requirements and regulations and maintains a level of compliance with this Agreement.

15.4 The Provider shall cooperate with external advisors to keep itself updated in accordance with Article 16.2. Applicable legislation, including whether new requirements and regulations emerge, or increased demands are placed on existing practices.

15.5 The Data Processor shall comply with the requirements set out in the Appendix to this Agreement called: "IT Security Policy". At least once a year, the Data Processor will update the requirements and will, if requested by the Data Controller, provide the updated requirements. Changes to the requirements must not disadvantage the Data Controller and should follow good industry practice.

ANNEX 3 - EVIDENCE OF COMPLIANCE

As part of the Data Processor's demonstration to the Data Controller of compliance with its obligations under Clause 4 of the Data Processing Agreement, the following items shall be performed and complied with.

16 GENERAL DOCUMENTATION FOR THE CONTROLLER

16.1 The Data Processor is obliged to provide the following general documentation to the Data Controller upon written request:

a) declaration by the management of the Data Processor that, in processing personal data on behalf of the Data Controller, the Data Processor will ensure ongoing compliance with its obligations under this Data Processing Agreement.

b) The general documentation shall be provided within five working days of the Data Controller's written request to the Data Processor, unless otherwise specifically agreed. The preparation of documentation by the Data Processor shall be at the Data Processor's own expense.

17 PHYSICAL MEETING WITH THE DATA PROCESSOR

17.1 The Data Processor shall, upon written request, attend a physical meeting at the premises of the Data Processor or the Data Controller, at which the Data Processor shall be able to provide details of compliance and how compliance is ensured. The request for a meeting shall be made with at least 14 days' notice.

17.2 Such a meeting shall be charged at the applicable hourly rate.

18 OTHER

18.1 The above points shall not be deemed exhaustive, and the Data Processor shall therefore be obliged to take such additional actions and measures as are necessary for the demonstration of the Data Processor's obligation under point 3 of the Data Processing Agreement.

18.2 The Data Processor is not obliged to comply with a request from the Data Controller under this Annex 3 if the request is contrary to personal data law regulation. The Data Processor shall notify the Data Controller to the extent that it is the Data Processor's assessment that this is the case.

ANNEX 4 - SUB-DATA PROCESSORS

19 SUB-DATA PROCESSORS - GENERAL

19.1 The Data Controller hereby gives its consent to the use by the Data Processor of the sub-data processors shown on this link.