Data Processor Agreement

Data Controller: Customer located within the EU (the "**Data Controller**") and

	Data Processor:
Company:	Kudos To You AB
Reg.no.	559359-4913
City:	Stockholm
Country of registration:	Sweden

(the "**Data Processor**")

(separately referred to as a "**Party**" and collectively the "**Parties**")

have concluded this:

DATA PROCESSOR AGREEMENT

(the "Agreement")

regarding the Data Processor's processing of personal data on behalf of the Data Controller.

1. The processed personal data

1.1 This Agreement has been entered into in connection with the Data Controllers use of the Data Processor's services as part of the subscription and additional services as described in "Qdos2U.com Terms and Conditions – Single event" or "Qdos2U.com Terms and Conditions – Subscription" (the "Main Agreement").

1.2 The Data Processor processes the types of personal data on behalf of the Data Controller in relation to the relevant data subjects as specified in Schedule 1. The personal data relates to the data subjects listed in Schedule 1.

1.3 The Data Processor may initiate processing of personal data on behalf of the Data Controller after the Agreement enters into force. The processing has the duration as specified in the instructions in Schedule 1 of the Agreement.

1.4 The Agreement and the Main Agreement are interdependent and cannot be terminated separately. However, the Agreement may be replaced with another valid Data Processor Agreement without terminating the Main Agreement.

2. Purpose

2.1 The Data Processor must only process personal data for purposes which are necessary to fulfil the Data Processor's obligations and in doing so providing the services set out in the Main Agreement.

3. Obligations of the Data Controller

3.1 The Data Controller warrants that the personal data is processed for legitimate and objective purposes and that the Data Processor is not processing more personal data than required for fulfilling such purposes.

3.2 The Data Controller is responsible for ensuring that a valid legal basis for processing exists at the time of transferring the personal data to the Data Processor. Upon the Data Processor's request, the Data Controller undertakes, in writing, to account for and/or provide documentation of the basis for processing.

3.3 In addition, the Data Controller warrants that the data subjects to which the personal data pertains have been provided with sufficient information on the processing of their personal data.

4. Obligations of the Data Processor

4.1 All processing by the Data Processor of the personal data provided by the Data Controller must be in accordance with instructions prepared by the Data Controller, and the Data Processor is, furthermore, obliged to comply with any and all data protection legislation in force from time to time. If Union law or law of an EU Member State to which the Data Processor is subject stipulates that the Data Processor is required to process the personal data listed in Schedule 1, the Data Processor must inform the Data Controller of that legal requirement before processing. However, this does not apply if this legislation prohibits such information on important grounds of public interests. The Data Processor must immediately inform the Data Controller if, in the Data Processor's opinion, an instruction infringes the EU General Data Protection Regulation or the data protection provisions of an EU Member State.

4.2 The Data Processor must take all necessary technical and organisational security measures, including any additional measures, required to ensure that the personal data is not accidentally or unlawfully destroyed, lost or impaired or brought to the knowledge of unauthorised third parties, abused or otherwise processed in a manner which is contrary to data protection legislation in force at any time. These measures are described in more detail in Schedule 2.

4.3 The Data Processor must ensure that employees authorised to process the personal data have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality.

4.4 If so requested by the Data Controller, the Data Processor must state and/or document that the Data Processor complies with the requirements of

the applicable data protection legislation, including documentation regarding the data flows of the Data Processor as well as procedures/policies for processing of personal data.

4.5 Taking into account the nature of the processing, the Data Processor must, as far as possible, assist the controller by appropriate technical and organisational measures, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights, as laid down in chapter 3 in the General Data Protection Regulation.

4.6 The Data Processor, or another Data Processor (sub-data processor) must send requests and objections from data subjects to the Data Controller, for the Data Controller's further processing thereof, unless the Data Processor is entitled to handle such request itself. If requested by the Data Controller, the Data Processor must assist the Data Controller in answering any such requests and/or objections.

4.7 If the Data Processor processes personal data in another EU member state, the Data Processor must comply with legislation concerning security measures in that member state.

4.8 The Data Processor must notify the Data Controller where there is an interruption in operation, a suspicion that data protection rules have been breached or other irregularities in connection with the processing of the personal data occur. The Data Processor's deadline for notifying the Data Controller of a security breach is 24 hours from the moment the Data Processor becomes aware of a security breach. If requested by the Data Controller, the Data Processor must assist the Data Controller in relation to clarifying the scope of the security breach, including preparation of any notification to the relevant Data Protection Agency and/or data subjects.

4.9 The Data Processor must make available to the Data Controller all information necessary to demonstrate compliance with article 28 of the General Data Protection Regulation and the Agreement. In this connection the Data Processor allows for and contributes to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

4.10 In addition to the above, the Data Processor must assist the Data Controller in ensuring compliance with the Data Controller's obligations under article 32-36 of the General Data Protection Regulation. This assistance will take into account the nature of the processing and the information available to the Data Processor.

5. Transfer of data to sub-data processors or third parties

5.1 The Data Processor must comply with the conditions laid down in article 28, paragraph 2 and 4 of the General Data Protection Regulation to engage another Data Processor (sub-data processor). This implies that the Data Processor does not engage another Data Processor (sub-data processor) to the

performance of the Agreement without prior specific or general written approval from the Data Controller.

5.2 The Data Controller hereby grants the Data Processor a general power of attorney to enter into agreements with sub-data processors. The Data Processor must notify the Data Controller of any changes concerning the addition or replacements of sub-data processors no later than 30 days prior to a new sub-data processor commencing processing of the personal data. The Data Controller can make reasonable and relevant objections against such changes within 14 days from receiving notification. If the Data Processor continues to wish to use a sub-data processor that the Data Controller has objected to, the Parties have the right to terminate the Agreement, cf. clause 7.

5.3 When the Data Controller has approved that the Data Processor can use a sub-data processor the Data Processor must impose the same obligations on the sub-data processor as set out in the Agreement. This is executed through a contract or another legal act under EU law or the law of a Member State. It must be ensured, e.g., that sufficient guarantees are provided from the sub-data processor to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the General Data Protection Regulation ("back-to-back" terms).

5.4 If the sub-data processor fails to fulfil its data protection obligations, the Data Processor remains fully liable to the Data Controller for the performance of the sub-data processor's obligations.

5.5 Disclosure, transfer and internal use of the Data Controller's personal data to third countries or international organisations may only take place in accordance with documented instructions from the Data Controller – unless stipulated by EU law or the law of a Member State to which the Data Processor is subject. If so, the Data Processor must notify the Data Controller of this legal requirement before processing, unless the law prohibits such notification for important grounds of public interests.

5.6 If the personal data stipulated in Schedule 1 is transferred to sub-data processors outside EU/EEA, it must, in the said agreement, be stated that the data protection legislation applicable in the Data Controller's country applies to sub-data processors. Furthermore, if the receiving sub-data processor is established within the EU/EEA, it must be stated in the said data processor agreement that the receiving EU country's specific statutory requirements regarding data processors, e.g., concerning demands for notification to national authorities must be complied with.

5.7 The Data Processor is obliged to enter into written data processor agreements with sub-data processors within the EU/EEA. As for sub-data processors outside the EU/EEA, the Data Processor must ensure the sufficient transfer mechanisms and enter into a sub-data processor agreement by entering into standard agreements in accordance with the EU Commission's Standard Contractual Clauses ("Standard contracts") based on 2021/914/EU of 4 June 2021.

5.8 At the time of the signature of this Agreement, the Data Processor engages the sub-data processors listed in Schedule 3.

6. Liability

6.1 The Parties' liability is governed by the Main Agreement.

6.2 The Parties' liability in damages under this Agreement is governed by the Main Agreement.

7. Effective date and termination

7.1 This Agreement becomes effective at the same time as the Main Agreement. In the event of termination of the Main Agreement, this Agreement will also terminate. However, the Data Processor remains subject to the obligations stipulated in this Agreement, as long as the Data Processor processes personal data on behalf of the Data Controller.

7.2 Upon termination of the processing services the Data Processor is obliged to, upon request of the Data Controller, delete or return all personal data to the Data Controller, as well as to delete existing copies, unless retention of the personal data is prescribed by EU or national law.

8. Governing law and jurisdiction

8.1 Any claim or dispute arising from or in connection with this Agreement must be settled by a competent court of the first instance in the same jurisdiction and with the same choice of law as stated in the Main Agreement.

9. Signatures

On behalf of the Data Controller:

_____

[Name] [Title]

On behalf of the Data Processor:

Linus Lancin CEO

Schedule 1

Categories of data subjects, Types of personal data and Instructions

1. Categories of data subjects:

• The Data Processor will be processing contact-information on Data Controller's actual, potential or former employees and collaboration partners.

• The Data Processor put its system for the disposal of the Data Controller as a hosted service, and it is not possible for Data Processor to determine all categories of data subjects. If the Data Controller host data on further categories of data subjects with the Data Processor, it is the Data Controller's obligation to register this information.

2. Types of personal data:

• Contact and identification information including e-mail

• Usernames

• Analytics and usage data

• Order-history and information

• Contracts

• Communication

• Support

• Pictures

• Additional types of personal data may occur

3. Instructions

Service

The Data Processor may process personal data concerning the data subjects with the purpose to deliver, develop, manage, administrate and manage the services of the Main Agreement, including ensuring stability and uptime of our servers and meet legal requirements.

Retention period

The personal data stored/hosted in our systems are deleted or anonymized within a reasonable time after the Data Controller has completely terminated the Main Agreement. Exceptions are data where there is a legal requirement for the Data Processor to save it longer. This type of data will typically be deleted within eight weeks but can be deleted earlier. Other types of data that are stored in logs etc. will be deleted after a reasonable time, typically within 8 weeks, after which they are deleted at the Data Processor.

Location of processing

Processing of personal data covered by the Agreement must not be done without the Data Controller´s prior written consent at locations other than the address of the Data Processor and the address of the sub-data processors as listed in Schedule 3.

Schedule 2

Security Measures

Data Processor is maintaining the solution and data using the security solution provided by the Hosting company, defined in Schedule 3. When the Data Controller and business users are accessing the data, the access is controlled on data row and user level.

Schedule 3

List of sub data processors

Supplier	Location	Function	Updated
one.com Group AB	DK	Datacenter	2023-01-24