Data Processor Agreement

Data Controller: Customer located within the EU
(the “Data Controller”)

and

	Data Processor:
Company:	One.com Group AB
Reg.no.	559205-2400
City:	Malmö
Country of registration:	Sweden

(the "Data Processor")

(separately referred to as a “Party” and collectively the “Parties”)

have concluded this

DATA PROCESSOR AGREEMENT - DPA
(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 Processors services as part of the subscription and additional services as described in “One.com Terms and Conditions” (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 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 Processors 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.

3.4 In case the Data Controller instructs a sub-Data Processor, appointed in accordance with clause 5.1 directly, the Data Controller must immediately inform the Data Processor hereof. The Data Processor shall not in any way be liable for any processing carried out by the sub-Data Processor in accordance with such instructions.

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 these instructions from 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 European Union law or law of a EU Member State to which the Data Processor is subject stipulates that the Data Processor is required to process the personal data listed in clause 1.2, 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 a 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 specified in clause 1.2 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 Danish data protection legislation in force at any time. These measures are described in more detail in Schedule 1.

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 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 consider 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 approval 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. The Data Controller can make reasonable and relevant objections against such changes. If the Data Processor continues to wish to use a sub-Data Processor to which the Data Controller has objected, the Parties have the right to terminate the Agreement and, if applicable, the Main Agreement with a shorter notice, cf. 7.2. During this period the Data Controller must not require that the Data Processor does not use the sub-Data Processor in question.

5.3 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, i.e., 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 liable to the Data Controller for the performance of the sub-Data Processor's obligations.

5.5 The Data Processor must, on behalf of the Data Controller, enter into Data Processor agreements with sub-Data Processors within the EU/EEA. As for sub-Data Processors outside the EU/EEA, the Data Processor must enter into standard agreements in accordance with Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries ("Standard contracts").

5.6 The Data Controller hereby grants the Data Processor a general power of attorney to enter into standard contracts with sub-Data Processors outside the EU/EEA on behalf of the Data Controller.

6. Liability

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

6.2 The Parties' liability for 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.

7.2 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.

In the situation as described under clause 5.2, the parties have the right to terminate the Main Agreement and the Agreement with a notice of 1 (one) month ending at the end of a month.

7.3 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 as stated in the Main Agreement.

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 customers and or members, employees, suppliers, business and collaboration partners and affiliates.
- The Data Processor put its system for the disposal of the 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
- IP-addresses
- Domain-names
- Usernames
- Membership information
- 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.

Security

The Data Processor shall ensure the confidentiality, integrity and availability of personal data. The Data Processor shall implement systematic, organisational and technical measures to ensure an appropriate level of security, taking into consideration the state, art and cost of implementation in relation to the nature of personal data and the risk of the processing.

The Data Processor shall provide a high level of security in its services and products. This security is provided through technical, organisational and physical security measures which include:

- Colocation facilities and offices are protected by appropriate access controls that ensure that only authorised staff have access.
- Relevant antivirus protection is in place.
- Access and login are role-based or individual based and staff and systems do not have more access than is necessary to perform their tasks.
- Backup of systems that process personal data.
- Changelogs.
- Communications over the internet between systems that handle personal data are encrypted.
- Classification of personal data to ensure implementation of security measures that correspond to the risk assessment.
- Use of systems and processes that help in improving the security in the handling of personal data.

The Data Processor is justified to make further decisions about the necessary technical and organisational security measures that must be implemented to ensure the appropriate security level regarding the personal data.

Retention period

Personal data stored/hosted in our systems are deleted or anonymised 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.

Location of data

Personal data stored/hosted in the Data Processors systems are hosted in data centres in Denmark. The Data Controller hereby authorises the Data Processor to move data to other data centres within the European Union if the Data Processor finds this relevant and if the same level of security and uptime can be ensured.

Inspection of Data Processor

The Data Processor must once every year at its own expense obtain an audit/inspection report from a third party regarding the Data Processor's compliance with this Agreement and Schedules.

Since the systems of the Data Processor are used by multiple Data Controllers the Data Controller grants for security reasons the Data Processor the authority to determine that the audit should be performed by a third-party inspector or auditor that the Data Processor selects.

If the Data Controller does not accept the neutral third-party chosen by the Data Processor the customer may choose another third-party together with the Data Processor.