**DATA PROTECTION AGREEMENT (neutraali)**

Sopimuspohja on tehty neutraalista näkökulmas­ta tilanteeseen, jossa kaksi yritystä käsittelee yhteistoiminnassaan henkilötietoja ja ne ovat näin ollen velvoitettuja tekemään EU:n tietosuoja-asetuksen (GDPR) mukaisen sopimuksen henkilötietojen käsittelystä. Tämä sopimuspohja toimii pääsopimuksen (toimitussopimus) liitteenä.

Sopimuspohjan kaikki kohdat tulee tarkistaa ja muuttaa vastaamaan käytännön tilannetta ja viimeisintä lainsäädäntöä; on myös huomioitava, että yhden sopimuskoh­dan muuttaminen yleensä vaikuttaa myös sopimuksen muihin lausek­keisiin ja lisämuutokset ovat tällöin tarpeen.

**HUOM.! Tämä sopimuspohja ei sovellu käytettäväksi käytännön tilan­teisiin ilman sopimusjuridisen asiantunti­jan tarkistusta ja kor­jauksia.**

*Draft 0.1– \_\_.\_\_.20­­\_\_*

**DATA PROTECTION AGREEMENT**

This Agreement(hereinafter the “Agreement”), dated this \_\_ day of June, 20\_\_, is made by and between Softafirma Oy, a Finnish corporation having offices as Pääkatu 1, 00100 Helsinki, Finland (hereinafter the “Processor”), and Ostajayhtiö Oy, a Finnish corporation having offices as Sivukatu 2, 00200 Helsinki, Finland (hereinafter the “Controller”).

1. Background

1.1 The Processor processes personal data on behalf of the controller. The Controller has chosen the Processer as a service provider according to the due diligence obligations as outlined in Art. 28 GDPR. In order for processing to be carried out in legal compliance, the Controller must give the Processor written instruction to carry out the processing on its behalf. This Agreement contains the intentions of the parties and particularly the will of the Controller to commission processing in the context of Art. 28 GDPR. The Agreement also regulates the rights and obligations of the parties in connection to the processing.

1.2 This Agreement is a supplementary agreement to the ICT Purchase Contract between the parties regarding a SaaS Service, which *enable Customers to xyz and abc* **(“Master Contract”**).

1.3 Where this Agreement uses the term “data processing” or “processing” (of data), this refers in particular to the collection, recording, storage, adaptation or use of personal data (see Art. 4 No. 2 GDPR).

1. Scope of the Contract

Where the Processor receives personal data belonging to the Controller and/or collects, processes or uses personal data for the Controller, the regulations of this Agreement are to be applied. The Processor processes personal data solely on behalf of the Controller and subject to the Controller’s instruction. Details regarding the type and function of the intended data processing, the type of personal data affected, as well as the categories of data subjects can be found in the Master Contract as well as in **Appendix 1** to this Agreement.

1. Rights and Obligations of the Controller

3.1 The Controller is responsible for the processing of the data bringing processed through the Processor on the behalf of the Controller.

3.2 The Controller is solely responsible for the protection of rights of data subjects. Rights of data subjects are enforceable against the Controller.

3.3 The Controller has the right to submit instructions regarding the type and purpose of the processing orally, in text format (e.g. by email) or in writing. Oral instructions must be confirmed in writing or in text format by the Processor without undue delay.

3.4 The Controller can name persons that are entitled to give instructions.

3.5 The Controller shall inform the Processor without undue delay if an error or an irregularity is found in connection with the processing of personal data through the Processor.

1. Obligations of the Processor

4.1 The Processor processes personal data solely subject to the instruction of the Controller and within the scope of the Agreement. The type and purpose of the processing are solely determinable by the instructions of the Controller. Instructions given by the Controller are to be documented by the Processor in a manner that is safeguarded from potential future manipulation. The instructions of the Controller are laid down in **Appendix 1**. Any processing that occurs outside of this is forbidden by the Controller, except where;

1. the Controller has agreed to the processing in writing – this is particularly true for a transfer to third parties, or
2. the processing is an obligation through the laws of the European Union or a Member State.

4.2 The Processor must support the Controller in its obligations to meet the requests of data subject’s rights. This includes in particular the obligation to correct, to delete or to restrict personal data, where the Controller has requested this in the Agreement or through instructions.

4.3 The Processor will comply with the applicable data protection law regulations. In particular, the Processor will not process data that is not generally accessible without authorization, will not retrieve data or keep data available through automatic procedures, nor will the Processor or another create data through automated or non-automated processing.

4.4 The Processor must facilitate potential organized data protection audits and audits that may occur through the relevant supervisory authority. In particular, the Processor has the obligation to share accurate, complete and timely information with the supervisory authority, to facilitate possible assessments (or audit) measures, as well as to implement measures assigned by the supervisory authority to remedy deficiencies in the technical and organizational measures.

The Processor will inform the Controller without undue delay if the supervisory authority contacts the Processor within the scope of its data protection audit or supervisory powers.

4.5 The Processor will support the Controller (or, where applicable, the Data Protection Officer) in carrying out of the Controller’s audits and will cooperate in the complete and timely completion of the audit. The Processor will support the Controller (or, where applicable, the Data Protection Officer) and its agents in documenting compliance with the agreed upon technical and organizational measures.

4.6 The Processor may create copies of the personal data and the data carrier where (i) the Controller has agreed to it in writing in advance, (ii) it is explicitly stated in this Agreement or in the Master Contract, or (iii) it is necessary for the purposes of this Agreement.

4.7 Documents containing personal data that are no longer required may only be destroyed with the advance agreement of the Controller. In exceptional cases as defined by the Controller, storage for the Controller or transfer to the Controller can occur.

4.8 The Processor confirms that it has appointed a Data Protection Officer in cases where this is a legal requirement, and that the Controller has been made aware of this in writing, or, where changes occur, in text form (e.g. email).

4.9 The Processor guarantees that, in the scope of the instructed processing of personal data, all agreed upon measures will be taken. He guarantees that the processed data will be kept separate from other data banks.

4.10 The Processor is required to operate its business and its business processes in such a way that the data, which he is commissioned by the Controller to process, is kept in a manner that provides the necessary safety, that it is protected from the unauthorized perusal by third parties and from perusal by unauthorized employees. If the Processor wishes to submit changes to the technical and organizational measures that are responsible for the safety of the data, these must first be agreed to by the Controller.

4.11 The Processor will inform the Controller without undue delay if a submitted instruction is, in the view of the Processor, in breach of legal requirements. The Processor is entitled to suspend the relevant instruction(s) until such a time that they are confirmed or changed by the Controller.

4.12 The Processor is required to inform the Controller without undue delay after becoming aware of every breach of data protection law regulations or of the contractual agreements and/or of the Controller’s submitted instructions, as well as of every relevant data protection law operational disturbance and/or irregularity in the processing of personal data that occurs in the processing of data through the Processor or though others employed by the Processor in relation to the processing. This applies particularly in relation to the Controller’s possible obligations to inform under Art. 33 and 34 GDPR. The Processor guarantees to assist the Controller without undue delay in fulfilling its obligations under the obligations under Art. 33 and 34 GDPR.

In particular, the Processor will report all breaches of the safety of the Controller’s personal data without undue delay, as soon as such a breach is known to the Processor.

Potential deficiencies in the commissioned processing must be remedied without undue delay, and through the provision of written evidence from the Processor.

4.13 The processing of data on behalf of the Controller outside the Processor’s business premises or through Subcontractors is only possible with the Controller’s permission. Processing data for the Controller in private premises is not permitted.

4.14 The Processor will appropriately label the data that is being processed on behalf of the Controller. Where the data is being processed for more than one purpose, the Processor will label the data with the respective purposes.

4.15 The Processor will assist in creating a record of processing activities. He will inform the Controller of the necessary details in an appropriate manner.

4.16 The Processor should inform the Controller of the person(s) who are authorized to receive information regarding processing activities.

The Person(s) authorized to receive information on behalf of the Controller are:

* xxxxxxxx

1. Scope of the Right to Instruct

5.1 The Controller retains a general right to instruct the Processor on the contents of this Agreement. The Controller has the right to submit additional instructions to the Processor at any time regarding the purpose, type and scope of the data for processing. Instructions that require a change to the purpose, type and scope of processing or to the types of data and the category of affected data subjects in accordance with **Appendix 1**, must be confirmed in writing. The Processor should be given an appropriate deadline for implementing the instruction.

5.2 Regulations about potential payment for excess work, which may occur by means of the additional instructions made by the Controller, remain unaffected.

1. Relationship with Subcontractors

6.1 The commissioning of a Subcontractor by the Processor is only permissible with prior written confirmation by the Controller.

6.2 The Processor must be diligent in its choice of Subcontractor, and prior to the commissioning, must assess whether the Subcontractor can fulfill the agreed contractual terms between the Processor and the Controller. In particular, the Processor must initially, and regularly for the duration of the contractual relationship, assess whether the Subcontractor has met the necessary technical and organizational measures for the protection of personal data under Art. 32 GDPR. The result of this assessment must be documented by the Processor, and, when requested, must be furnished to the Controller.

6.3 The Processor must contractually assure that the regulations of this Agreement, and where appropriate, additional instructions given by the Controller, are also binding on the Subcontractor. The Processor must regularly assess that these requirements are being met.

6.4 Transferring data to the Subcontractor is only permissible once the Subcontractor has met the requirements laid out in Paragraphs 8 and 12 of this Agreement.

6.5 The requirements on the Subcontractor must be made in writing. The Controller must be copied into this written obligation upon request.

6.6 Sub-contractual relationships, where the Processor uses third-party service providers as support for fulfilling its duties are not to be considered as Subcontractors for the purposes of this contract. Examples include telecommunication service providers or cleaning service providers. However, the Processor is required to guarantee the security of the Controller’s data, and to make appropriate and legal contractual agreements with third party service providers, as well as to take measures to assess this.

1. Right of Assessment

7.1 The Controller, or, where appropriate, the Data Protection Officer and his agents have the right to assess compliance with legal requirements of data protection law, particularly the technical and organizational safety measures taken by the Processor, and/or compliance with the contractual regulations agreed upon by the parties, and/or compliance with the Controller’s instructions by the Processor prior to the commencement of the commissioned processing and at any time for the duration of the Agreement in the necessary scope.

7.2 The Processor must share information with the Controller where this is necessary to carry out an assessment as described in point 7.1 above.

7.3 The Controller can request viewing rights for the data that is being processed by the Processor on the Controller’s behalf, as well as for the data processing systems and programs in implementation.

7.4 The Controller can carry out the assessment as described in point 7.1 above at the Processor’s place of business at any time during normal working hours with appropriate advance notice. The Controller will ensure that such an assessment will only take place where necessary, to avoid disturbances of the Processor’s business operations.

1. Data Integrity & Confidentiality

8.1 The Processor’s employees are bound to the principle of protection of data integrity and confidentially under GDPR. The Processor is therefore required to observe the same rules of data secrecy as those that apply to the Controller.

8.2 The Processor guarantees that he is familiar with the applicable data protection laws, and that he is aware of how to apply these. Furthermore, the Processor guarantees that the employees carrying out the processing will be made aware of the measures of data protection and that they will be bound to data confidentiality. Personal data may only be made accessible to employees of the Processor who require the data to fulfill this Agreement. The Processor must provide the Controller with these confidentiality agreements upon request.

1. Protection of Data Subjects’ Rights

9.1 The Controller is solely responsible for the protection of data subjects’ rights.

9.2 Where the Controller requires cooperation from the Processor in its duty to protect data subjects’ rights – particularly in the informing, correction, transferability, restriction or deletion of the data – the Processor will meet the requests of the necessary measures to be taken without undue delay through the instruction of the Controller. The Processor will inform the Controller without undue delay if a data subject contacts the Processor to request information, correction, transferability, restriction or deletion of his/her data.

1. Confidentiality

10.1 Both parties are required to handle all information obtained in connection with the carrying out of this Agreement confidentially without time limitation and to only in use the data for the carrying out of this Agreement. No party is entitled to share or partially share this information with others, or to use is for purposes other than those listed.

10.2 This obligation does not apply to information that the parties have demonstrably received from third parties that are not bound to confidentiality, or to information that is publicly available or that will become publicly available.

1. Payment

The Processor’s activities shall be compensated on hourly basis in accordance with the Processor’s current consultancy rates.

1. Technical and organizational measures for data security

The Processor guarantees the Controller that shall implement technical and organizational security measures as listed in Art. 32 GDPR, that are necessary for compliance with the applicable data protection regulations. The exact measures to be taken are listed in the data protection and security concept in **Appendix 2**. The Processor will regularly review the compliance with the technical and organizational measures. For assessment purposes, the Processor will submit documentation regarding the technical and organizational measures that have been met to the Controller’s Data Protection Officer and his agents. The Processor shall maintain and regularly update this data protection and security concept, with changes to be agreed to in writing by the Controller.

1. Liability

Liability within the contractual relationship applies as expressed in the Master Contract.

1. Termination

14.1 Upon termination of this Agreement, or upon the instruction of the Controller, the Processor must return all documents, data and results created from processing or usage that are in connection with this Agreement to the Controller within 14 days. The Processor’s data carriers must, in accordance with data protection law regulations, be deleted and/or destroyed. This also affects possible backups. The deletion is to be documented in an appropriate manner. Test or excessive materials are, in accordance with data protection law regulations, to be destroyed and/or to be physically deleted without undue delay.

14.2 The Controller has the right to inspect the complete and contractually agreed upon return and deletion of the data stored by the Processor. This can also occur in the form of an inspection of the data processing facilities at the business premises of the Processors. Appropriate notice will be given for an on-site inspection.

1. Miscellaneous

15.1 The Controller retains all rights over the personal data, data carriers as well as all copies thereof. Should the property and the rights of the Controller be jeopardized by the actions of third parties (through confiscation or seizure), through insolvency procedures or other occurrences, the Processor must inform the Controller without undue delay. The Controller will inform the creditors without undue delay that the confiscation is of data that is being processed on his behalf.

15.2 The Processor’s obligations due to legal requirements or supervisory authorities or court orders remain unaffected by this Agreement.

15.3 The Agreement is enforceable with the commencement of the Master Contract, and will be binding until the Master Contract has been terminated. If processing of personal data is necessary after the termination of the Master Contract for the cessation of the Master Contract or due to legal requirements, for example for the publication of personal data, this Agreement will be binding until the cessation is complete.

15.4 Additional agreements must be made in writing.

15.5 Should aspects of this Agreement contradict other binding agreements between the Processor and Controller, the regulations of this Agreement shall be binding.

15.6 Should individual parts of this Agreement be unenforceable, this does not affect the enforceability of the other regulations of this Agreement.

............................................................... ...................................................................

Date Date

............................................................... ....................................................................

(Controller) (Processor)

# Appendix 1

# Appendix 2