Data Processing Appendix

This Data Processing Appendix (the "**Appendix**") is attached to and forms part of the Supplier General Terms and Conditions (the "**Agreement**") between Nebula Oy ("**Supplier**") and customer ("**Customer**")

BACKGROUND

(a) Pursuant to the Agreement, Supplier provides Services, including but not limited to Hosting Services and/or Support (as defined in the Agreement) to Customer.

(b) The Services may be used to store and/or otherwise Process data, including Personal Data of the Customer. The Customer is the data Controller of such Personal Data Processed in connection with the Services. Supplier is the Processor of such Personal Data.

(c) The parties desire to address their compliance obligations under applicable personal data protection legislation (Laws).

Supplier and Customer agree as follows:

The Parties agree to comply with the following provisions with respect to any Personal Data stored and/or otherwise Processed in the Services.

1. DEFINED TERMS

Capitalized terms not otherwise defined in this Appendix shall have the meaning given to them in the Agreement. For the purposes of this Appendix, the following additional definitions apply:

"Controller" means Customer or Customer's client, who determines the purposes and means of the Processing of Personal Data.

"Laws" means the any applicable national data protection laws, the EU Data Protection Regulation (2016/679, "GDPR") when applicable as of 25 May 2018 and any future data protection legislation as applicable from time to time.

"Model Clauses" means the standard contractual clauses approved by European Commission for transfers of personally identifiable data from controllers in the EU to processors in third countries (Decision 2002/16/EC).

"Supplier Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with Supplier, but only for so long as such control exists. As used in this definition, "Control" means the right to control more than fifty percent (50%) of the voting interests of the entity.

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processor" means Supplier, who Processes Personal Data on behalf of the Customer and/or Controller.

"Processing" or "Process" means any operation or set of operations that is performed upon Personal Data.

Sub-Processor: a processor contracted by Supplier to perform Processing hereunder on behalf of Supplier, Customer and/or Controller.

2. OBLIGATIONS OF SUPPLIER

2.1 Supplier's Role in the Processing of Customer's Personal Data. Supplier does not determine the types of Personal Data stored by Customer and/or Controller in the Services or how such data is classified, accessed, exchanged, or otherwise Processed. Supplier shall Process Personal Data only on Customer's and/or Controller's behalf and only to the extent and in such a manner as is necessary for the purposes specified by and in accordance with this Appendix and the Agreement or as otherwise instructed by the Customer from time to time. Such Customer instructions shall be documented in the applicable Order, Services Description, a customer support ticket, or other written communication.

Where Supplier reasonably believes that a Customer instruction is contrary to: (i) applicable law and regulations, and/or (ii) the provisions of the Agreement or Appendix, Supplier will inform the Customer without undue delay and is authorized to defer the performance of the relevant instruction until it has been amended by Customer or is mutually agreed by both Customer and Supplier.

2.2 Data Security Supplier shall implement and maintain appropriate technical and organizational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing; the risk of varying likelihood and severity for the rights and freedoms of natural persons, as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data transmitted, stored or otherwise processed.

The employed data security measures are defined in Supplier´s minimum security practices detailed at http://www.nebula.fi/. Customer is responsible to inform Supplier of all issues (including special risks or categories of Personal Data) which require additional technical or organizational security measures to be defined and agreed in the Agreement.

Where Supplier requires access to Personal Data for the purpose of fulfilling its obligations under the Agreement or Appendix, it shall limit such access and Processing to the Qualified Personnel. For the purposes of this sub-section, the "**Qualified Personnel**" means those employees and/or agents, consultants, subcontractors, or other third parties (i) who are engaged by Supplier so that it may fulfill its obligations to Customer under the Agreement or Appendix, and (ii) who are subject to confidentiality and security obligations that are the same or substantially similar to the confidentiality and security obligations set forth in the Agreement and Appendix.

2.3 Requests from data subjects or authorities. Taking into account the nature of the Processing, Supplier shall assist and support the Controller (at Controller's expense) with appropriate technical and organizational measures, insofar as this is possible, so that the Controller can fulfil its obligation to respond to requests from data subjects.

Supplier shall notify the Customer without undue delay in writing:

- of any communication received from an individual relating to (i) an individual's rights to access, modify, correct, delete, or block his or her Personal Data, and (ii) any complaint about Customer's and/or Controller's Processing of Personal Data;
- to the extent not prohibited by law, of other judicial or administrative order or proceeding seeking access to, or disclosure of, Personal Data;
- to the extent not prohibited by law, of any complaint, notice or other communication that relates to Customer's and/or Controller's compliance with data protection and privacy law and the Processing of Personal Data.

2.4 Supplier's Compliance with Law. Supplier shall comply with the privacy and security laws applicable to its own operations and provision of the Services under the Agreement and its obligations under this Appendix. However, Supplier is not responsible for compliance with any laws applicable to Customer or Customer's industry and/or Controller or Controller's industry that are not generally applicable to information technology service providers. Where required by applicable law, Supplier shall appoint a data protection officer who shall discharge its function in accordance with applicable law. The data protection officer's details shall be provided to the Customer upon request.

Supplier shall maintain necessary records and at the request of Customer, make available to Customer all information necessary to demonstrate compliance with its obligations under this Appendix and the Laws.

2.5 Audit. Supplier shall engage qualified third-party auditors to perform examinations of its Services and Processing of Personal Data in accordance with industry standards. Subject to Supplier's policies and the terms of the Agreement, and only to the extent not covered by the independent audit reports set forth above, Supplier will agree that the Customer or its representatives may at Customer's expense perform physical and/or electronic reviews of the security of Services and Processing of Personal Data or evaluate and monitor Supplier's compliance with its security obligations set forth under the Appendix.

At the expiry of the Agreement or Service, the Supplier shall at Customer´s instructions either delete or return to Customer all the Personal Data. If the Customer has not given any instructions within 30 working days from the expiry of the Agreement of Service, Supplier shall delete all the Personal Data, unless required to retain Personal Data by the Laws.

2.6 Supplier's Assistance with Customer's or Controller's Compliance Requirements. During the term of Customer's Agreement with Supplier, Customer may request that Supplier assist Customer and/or Controller in complying with Customer's and/or Controller's obligations under applicable data protection or privacy law and regulations provided that (i) such obligations are relevant to the Services, (ii) such obligations are commercially reasonable, and (iii) if Supplier agrees to so assist, it shall be at the Customer's expense.

3. OBLIGATIONS OF CUSTOMER AND/OR CONTROLLER

3.1 Customer's and/or Controller's Compliance. The Controller shall determine the types of Personal Data stored by Customer and/or Controller in the Services or how such data is classified, accessed, exchanged, or otherwise Processed and ensures that all the data subjects of the Personal Data have been provided with all appropriate notices and information about Processing, and that it has the necessary rights and consents to process Personal Data. The Controller is responsible for drafting a record on Processing.

In relation to Customer´s and/or Controller's Processing of the Personal Data and its use of the Services, Customer and/or Controller is responsible for the integrity, security, maintenance

and appropriate protection of Personal Data, and for ensuring its compliance with any applicable privacy, data protection and security law and regulation.

3.2 Technical and Organizational Measures. Customer and/or Controller is solely responsible for implementing and maintaining security measures and other technical and organizational measures appropriate to the nature and volume of Personal Data that Customer and/or Controller stores and/or otherwise Processes using the Services. Customer and/or Controller is also responsible for the use of the Services by any of its employees, any person Customer and/or Controller authorizes to access or use the Services, and any person who gains access to its Personal Data or the Services as a result of its failure to use reasonable security precautions, even if such use was not authorized by Customer and/or Controller. Customer may purchase supplementary services from Supplier in order to meet its obligations under this Sub-section 3.2.

4 MANAGEMENT OF DATA SECURITY INCIDENTS

Each Party agree to notify the other Party without undue delay, if it becomes aware of any unauthorized use of Services, Customer's account or any other breach of Personal Data related to the Services. The notification shall include following information - if obtainable:

- the circumstances giving rise to the Personal Data Breach
- a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Each Party shall in its own area of responsibility investigate all causes for the breach and take appropriate actions to end the breach, mitigate the effects and prevent further similar breaches. The Parties shall document and report to the other Party the results of its investigation and the actions taken. The Parties shall cooperate in the reasonable investigation of the incidents.

Customer and Supplier agree to cooperate as reasonably required to protect the Services, the Service environment, the system hosted in the Services, and any Personal Data in relation to any investigation of Service outages, security problems, and any suspected security breach.

5. SUB-PROCESSING

Supplier may need to engage Sub-processors to provide Services and Support to Customer. Customer hereby gives its specific consent to Supplier ´s use of Supplier Affiliates as its Sub-Processors.

In addition, Customer hereby gives its general consent to Supplier ´s use of other Sub-Processors on following conditions: Supplier will provide Customer with a list of Sub-Processor(s) used in the provision of Service in the Agreement or otherwise in writing. Supplier will inform Customer in advance on any new Sub-Processors. Customer shall notify Supplier about rejection of the new Sub-Processor promptly, but no later than fourteen (14) days after

receipt of Supplier ´s notice. Supplier may then terminate such part of the Agreement which the sub-processing would be related to by way of thirty (30) days' prior written notice.

Supplier will require Sub-Processors to conclude a written agreement and to comply with the data protection, security and confidentiality obligations applicable to Supplier under this Appendix and Agreement or obligations which provide for the same level of data protection.

Any Sub-Processing shall be strictly in accordance with the terms of the Agreement and this Appendix. Supplier remains responsible to Customer under the Agreement for Services performed by its Sub-processors to the same extent as if Supplier performed the Services itself.

6. DATA CENTER LOCATION AND DATA TRANSFER

Supplier's data centers reside in Finland where all Personal Data is primarily stored and processed. Supplier may however transfer Personal Data to any data center residing in EU/EEA or outside the EU/EEA to the extent described in the Service descriptions or agreed in the Agreement. Transfers of Personal Data to outside EU/EEA shall be subject to Model Clauses, which shall be appended to this Appendix, and form an integral part of this Appendix and supersede any conflicting terms or conditions in this Appendix and Agreement, or another transfer mechanism approved by the Laws.

7. CUSTOMER ACCOUNT INFORMATION

Personal Data that Supplier collects about Customer and/or Controller during the purchase, account sign-up, use or maintenance of Customer's account, shall be processed by Supplier in accordance with its then-current Privacy Statement, a current version of which is located at www.nebula.fi/.

8. LIMITATIONS OF LIABILITY

The limitations of liability in the Agreement shall apply also to this Appendix. Any administrative fines imposed, or damages ordered shall be paid by the Party that has failed in its performance of its legal obligations under this Appendix or the Laws, as decided by the relevant supervisory authority or competent court authorized to impose such fines or damages.

9. ORDER OF PRECEDENCE

To the extent that any provision of the Appendix conflicts with any provision of any other document(s) of which the Agreement comprises, the terms of the Appendix shall, as to the specific subject matter of the Appendix, take precedence over the conflicting term(s) of such other document(s).

10. GOVERNING LAW

Nothing in this Appendix amends the Governing Law section of the Agreement, which shall, for the avoidance of doubt, govern all claims brought under the Agreement and this Appendix.