DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA"**) is made a between the following parties:

Client's identification information is recorded in the Agreement (as it's defined in Focal's Terms of Service) between Client and Focal Technologies Ltd.
(hereinafter referred to also as "**Controller**")

Company name: Focal Technologies Ltd.
Business ID: 3235589-3
E-mail address: team@focal.inc
Address: Paasivuorenkatu 4, 00530 Helsinki
(hereinafter referred to also as "**Processor**")

This DPA sets out the terms and conditions for Personal Data Processing, including the relevant data security measures, that the Processor undertakes to abide when Processing Personal Data on behalf of Controller. In the course of providing the Service, Focal will process personal data only in accordance with the Agreement. Upon the Client's written request, Focal will destroy or return to the Client, such personal data, and destroy existing copies unless applicable EU, EU Member State or US law requires the storage of the personal data.

1. Definitions

This DPA uses the same definitions as in the Agreement, unless otherwise defined below.

1.1 "**Personal Data**" means any information relating to an identified or identifiable natural person, including an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.2 "**Data Subject**" means a natural person who can be identified, directly or indirectly, by the Personal Data.

1.3 "**Processing**" or "**to Process**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.4 "**Sub-processor**" means any third party engaged by the Processor, or its Sub-processor, to process Personal Data on behalf of the Controller.

1.5 “**SCC**” means the standard contractual clauses for the transfer of Personal Data to processors established in third countries, set forth in the European Commission Decision of 5 February 2010, or any such standard contractual clauses amending or replacing the SCC.

1.6 “**Data Protection Law**” means any applicable legislation protecting the personal data of natural persons, including in particular the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) (as amended and superseded from time to time), together with all applicable laws, rules, regulations, regulatory guidance and regulatory requirements from time to time in relation to data privacy.

2. Data Processing

2.1 The Controller shall be responsible for the lawful Processing of Personal Data and for fulfilling other obligations of a controller, as set out in Data Protection Law. The Controller shall also be responsible for informing the Data Subjects on the Processing of their Personal Data.

2.2 The Processor agrees to comply with Data Protection Law, and with any other applicable law to the extent it is not in conflict with Data Protection Law.

2.3 The Processor shall only Process Personal Data in accordance with the instructions stated in this DPA or any other documented instructions provided by the Controller from time to time. If EU or EU member state law imposes additional processing requirements, the Processor shall inform the Controller of such legal requirements before Processing, unless prohibited by applicable law on important grounds of public interest.

2.4 If the Processor lacks instructions which the Processor deems necessary in order to carry out an assignment from the Controller, or if the Controller’s instructions infringe Data Protection Law or other applicable law, the Processor shall notify the Controller without undue delay and await the Controller’s further instructions.

2.5 The Processor shall enable the Controller to access, rectify, erase, restrict and transmit the Personal Data Processed by the Processor. The Processor shall comply with any instruction related to the above without undue delay. If the Controller erases, or instructs the Processor to erase, any Personal Data held by the Processor, the Processor shall ensure that the Personal Data is erased so that it cannot be recreated by any party.

2.6 The Processor shall notify the Controller without undue delay as to any contacts with a supervisory authority, concerning or of significance for, the Processing of Personal Data carried out on behalf of the Controller. The Processor may not represent the Controller, nor act on the Controller’s behalf, against any supervisory authority or other third party.

2.7 The Processor shall assist the Controller in its contacts with any supervisory authority, including, upon the Controller's instruction, by providing any information requested by the supervisory authority. For the avoidance of doubt, the Processor may not disclose Personal Data or any information on the Processing of Personal Data without explicit instructions from the Controller.

2.8 If a Data Subject requests information from the Processor concerning the Processing of Personal Data, the Processor shall forward the request to the Controller and assist the Controller in responding to such request as obliged by Data Protection Law. The Processor shall assist the Controller by appropriate technical and organizational measures, taking into account the nature of the Processing. For the avoidance of doubt, the Processor shall have no right to invoice any costs incurred due to assistance provided to the Controller in responding to requests submitted by a Data Subject.

2.9 The Processor shall impose adequate contractual obligations regarding confidentiality and security upon its personnel which have been authorized to Process Personal Data.

2.10 The Processor shall assist the Controller in ensuring compliance with the Controller's obligations under Data Protection Law, e.g. assist with security measures, data protection impact assessments (including prior consultation), and in situations involving Personal Data breach.

2.11 The Processor shall maintain a record of all Processing activities carried out on behalf of the Controller. Upon the Controller's request, the Processor shall promptly make the record available to the Controller in a generally readable electronic format, including as a minimum the following information:

a) the name and contact details of the Processor, its authorized representatives, and if applicable, the Data Protection Officer (as defined in Data Protection Law) of the Processor;
b) where applicable, the name and contact details of any Sub-processor, its authorized representative, and Data Protection Officer of the Sub-processor;
c) the actual processing activities carried out by the Processor and/or Sub-processor on behalf of the Controller;
d) where applicable, transfers of Personal Data to a third country including the identification of that third country and suitable safeguards employed to ensure an adequate level of protection for the Data Subject; and
e) a general description of the technical and organizational measures employed to ensure an appropriate level of security.

3. Data Security

3.1 The Processor shall implement appropriate technical and organizational security measures to protect the Personal Data in accordance with Data Protection Law. In this regard, the Processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the level of risk associated with the Processing, implement appropriate technical and organizational measures to ensure data security, including inter alia as appropriate:

a) the pseudonymization and encryption of Personal Data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

3.2 When implementing appropriate technical and organizational security measures, the Processor shall observe relevant codes of conduct, industry best practice, and guidelines issued or approved by supervisory authorities.

4. Data Breaches

4.1 The Processor shall notify the Controller, in writing, without undue delay, and in any case within 48 hours, after the Processor has or should have become aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. The notification shall at least:

a) describe 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;
b) describe the likely consequences of the Personal Data breach; and
c) describe the measures taken or proposed to be taken by the Processor to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.2 The Processor shall immediately after becoming aware of data breach undertake prompt action to inspect the cause and effects of the data breach and carry out appropriate measures to end the breach, minimize the effects and prevent comparable breaches from occurring. The Processor shall document the results of the inspection, and the measures carried out, to the Controller.

4.3 The Processor shall cooperate with the Controller and ensure that the Controller has the documentation required by Data Protection Law and the competent data protection authorities at hand.

5 Sub-Processing

5.1 The Client agrees that Focal may process personal data in any country in which any of Focal' subcontractors maintain facilities, provided that (a) such processing fulfills all legal requirements set forth in the GDPR, and that (b) the provisions of these terms are observed.

6 Transfer of Personal Data Outside the EEA

6.1 Except where otherwise agreed between the Parties or further specified in this DPA, the Processor shall not transfer Personal Data to a country outside of the EEA.

6.2 The Processor does not primarily process data in non-EEA countries. However, it is possible that the service providers or sub-contractors of the Processor process personal data in non-EEA countries. In this case, the Processor try to secure the processing of personal data by the SCC whenever possible.

7 Indemnification

7.1 In accordance with Data Protection Law, if the Processor Processes Personal Data in breach of Controller's lawful instructions, this DPA or Data Protection Law, the Processor shall fully indemnify and hold the Controller harmless for losses, costs or damages resulting from claims by Data Subjects, due to the Processor's (or its Sub-processors') Processing of Personal Data. The Parties liability for administrative fines, imposed by relevant supervisory authority, shall follow the terms set out in Data Protection Law. Except for losses, costs or damages set out above, the Parties liability shall be stipulated in accordance with the DPA.

7.2 In case of claims by a Data Subject or financial penalties imposed by supervisory authorities or other competent authorities, the Controller shall, where this would not jeopardize the Controller's defense: (a) notify the Processor promptly in writing of any such potential or pending claims or penalties; (b) use reasonable endeavors to reduce or avoid such claims or penalties; (c) allow the Processor to comment on any response, settlement, defense or appeal in relation to such claim; and (d) to a reasonable extent provide the Processor with information in relation to the same. For the sake of clarity, the Controller will not be bound by any recommendations made by the Processor.

8 Settlement of disputes

8.1 This Agreement shall be governed by the laws of Finland, and any disputes will be settled at the District Court of Helsinki as the court of the first instance.

9 Term

9.1 Upon termination or expiry of the services relating to the Processing, the Processor shall return all Personal Data to the Controller in a structured, commonly used and machine-readable form. The Processor shall thereafter, in accordance with the provisions on erasure in Section 2.5, ensure that there is no Personal Data remaining with the Processor or any of its Sub-processors.

9.2 This DPA is applicable from the date of its execution and until all Personal Data is erased in accordance with Section 9.1 above.

This DPA has been executed electronically as the Agreement.