DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is made between Groups.io Inc.**,** with its principal place of business at 3130 Alpine Rd #288-263 - Portola Valley, Ca 94028, USA ("**Groups.io**") and _____, with its principal place of business at _____ ("**Provider**"). This DPA supplements the Customer Terms of Service agreement found at https://groups.io/static/tos between Groups.io and Provider (the "**Agreement**").

BACKGROUND:

Provider provides certain services to Groups.io in accordance with the Agreement (the "**Services**"). Provision of the Services involves the Processing of Personal Data by Provider. This DPA governs the Processing of Personal Data by Provider, in the course of providing the Services.

IT IS AGREED AS FOLLOWS:

1. Definitions

For the purpose of this DPA, unless otherwise defined in the Agreement, all capitalized terms used in this DPA shall have the meanings given to them below:

"**Controller**", "**Processor**", "**Personal Data**", "**Data Subject(s)**", "**Processing**" (the terms "**Process**", "**Processes**" and "**Processed**" are interpreted accordingly), "**Personal Data Breach**", "**Supervisory Authority**" shall have the meanings given to them in the Data Protection Laws.

"**Data Protection Laws**" means rules and regulations applicable with respect to the Processing of Personal Data under the Agreement and this DPA, notably resulting from the European General Data Protection Regulation no. 2016/679 dated 27 April 2016 ("**GDPR**"), as amended and supplemented, as the case may be, by the relevant EU Member States laws and regulations in which Groups.io directly or indirectly operates, and the Directive no 2002/58 or any other text that may replace it and/or as amended and supplemented, as the case may be, by the relevant EU Member States laws and regulations in which Groups.io directly or indirectly operates.

2. Data Protection Obligations

2.1. Compliance with Laws. Provider shall comply with Data Protection Laws.

2.2. Instructions. Provider shall only Process Personal Data (i) on behalf of Groups.io, (ii) further to written and documented instructions received from Groups.io, included, as the case may be, in the DPA and/or the Agreement (each, an "Instruction") and (iii) to comply with applicable Data Protection Laws. Provider warrants it has no reason to believe that the legislation applicable to it prevents it from fulfilling any Instruction.

2.3. If, in Provider's opinion, any Instruction were to (i) appear legally prohibited, (ii) to require material changes to Provider' performance of the Services, (iii) result in a likely violation of Data Protection Laws and/or (iv) appear inconsistent with the terms of the Agreement or this DPA, Provider shall immediately inform Groups.io of its inability to follow such Instruction, and any Processing described in the Agreement and/or the DPA. In this case, Groups.io may terminate the Agreement and this DPA, without prior notice and without any right to compensation.

2.4. Provider undertakes to keep and maintain adequate and complete documentation and record of Provider's Processing or use of Groups.io's Personal Data, in accordance with Data Protection Laws. Provider undertakes to perform, without limitation, any formality, request for authorization, approval, and data protection impact assessment, as may be prescribed by Data Protection Laws. In any case, Provider undertakes to comply with the principles of "privacy by design" and "privacy by default", as provided for in the Data Protection Laws.

2.5. Division of roles and responsibilities. Under this DPA, Provider shall Process Personal Data as Processor, and Groups.io shall act as Controller. Should Provider Process Personal Data outside the scope of this DPA, such as, without limitation, (i) for purposes of Processing other than those agreed in this DPA, (ii) for any Processing operation outside Groups.io's instructions, (iii) for any Processing performed for a duration other than as specified in Section 3 of this DPA, Provider shall be considered as Processor.

2.6. Use and Purpose Limitation. Provider shall not Process Personal Data for any purpose other than to perform the Services in compliance with the Agreement, this DPA and Instructions, and for the duration of the Agreement or otherwise indicated under relevant Instructions. In particular, and without prejudice to the foregoing, Provider shall not copy, use, reproduce, display, perform, sell, modify, destroy or transfer any Personal Data, works derived from Personal Data or anything that includes any Personal Data, to any third party, except as otherwise expressly set out in this DPA, the Agreement or any Instruction.

2.7. Limited disclosure. Provider shall not disclose Personal Data to any third party except as necessary to perform the Services or further to an Instruction. Provider shall further ensure that access to Personal Data to perform the Services will be granted only on a strict need-to-know basis to authorized personnel, including employees, contractors and agents, which shall be subject to appropriate confidentiality obligations, as well as provided with appropriate instructions and training on data protection principles and security. Provider also warrants that any person acting under its authority and having access to Personal Data for the provision of the Services shall process them according to the Instructions only.

2.8. Notification of Groups.io in case of disclosure requests / question. Provider shall notify Groups.io without delay upon – and in any event no later than twenty-four (24) hours after – becoming aware of (i) any legally binding request for disclosure of and/or request for access to Personal Data by a law enforcement authority unless otherwise prohibited under applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; (ii) any legally binding request, order or inspection activity by a Supervisory Authority or other competent authority relating to Personal Data or privacy protection; or (iii) any request or question received from Data Subjects in relation to their Personal Data, such as requests for access, rectification, portability or deletion of their Personal Data. Except in order to confirm that such request is properly directed to Groups.io, Provider shall not respond independently to any such questions and/or requests, unless otherwise expressly agreed in writing by Groups.io; in such case, Provider undertakes to comply with the processes and conditions set out by Groups.io to this effect.

2.9. Assistance to Groups.io. Provider shall timely assist Groups.io, through appropriate technical and organizational measures, to respond and act upon any requests made by a Supervisory Authority or a Data Subject under Data Protection Laws. More generally, Provider shall provide timely assistance to Groups.io, insofar as Provider is not prohibited to do so, for Groups.io to comply with its obligations under applicable Data Protection Laws. Upon Groups.io's request, Provider shall provide Groups.io with all cooperation and assistance needed to fulfil Groups.io's obligation under applicable Data Protection Laws to carry out a data protection impact assessment related to Groups.io's use of the Services, notably where the Services involve automated decision-making and profiling as well as any Processing activity performed on special categories of data pursuant to Article 9 of GDPR, geolocation data and/or any large scale Processing of Personal Data. Provider shall provide reasonable assistance to Groups.io in the cooperation or prior consultation with the relevant

Supervisory Authority in the performance of its tasks relating to this Article to the extent required under the relevant Data Protection Laws.

2.10. Security. Provider shall implement appropriate physical, technical and organizational measures to protect Personal Data against accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of personal data over a network, and against all forms of unauthorized or unlawful processing. Such measures shall ensure a level of security appropriate to the risk, including *inter alia,* as appropriate: (i) the pseudonymization and encryption of Personal Data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) 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 (iv) a process for regularly testing, assessing and evaluating the effectiveness of physical, technical and organizational measures in place for ensuring the security of any processing for the purpose of providing the Services. Provider shall in any event comply with any data security documentation that Groups.io may provide, from time to time. Security measures are described in Appendix 3 hereto and shall be regularly assessed and updated by the parties.

2.11. Notification of Personal Data Breaches. Provider shall notify Groups.io without delay upon –and in any event no later than twenty-four (24) hours after – becoming aware of any breach of this DPA or any Personal Data Breach (together, "**Breach**"). Provider shall timely document and provide Groups.io with all data and details relating to such breach and provide any necessary assistance to enable Groups.io to remedy any such breach and provide Groups.io with all reasonable assistance to provide notification of any such breach to any Supervisory Authority and/or the Data Subjects impacted by such Breach. In particular, and without prejudice to any other right or remedy available to Groups.io , Provider shall promptly following discovery or notice of a Breach, at its own costs and expenses, take (i) corrective action to mitigate any risks or damages involved with such Breach and to protect the Personal Data from any further use and/or access, (ii) evidence and document such Breach, in particular its context, date of occurrence, type, extent and data involved, as well as any elements pertaining to the diagnosis of the origin or the occurrence of such Breach, and the direct and indirect consequences of this Breach, and provide Groups.io with such evidence and documents, and (iii) any other actions that may be required by applicable Data Protection Laws as a result of such Breach, subject to Groups.io's prior written approval.

2.12. Return and Deletion of Personal Data. Upon expiration or termination of the Agreement, for any reason whatsoever, Provider shall, at the choice of Groups.io, within 15 (fifteen) days following the expiration or termination, (i) return all Personal Data Processed in the course of providing the Services and copies thereof to Groups.io, (ii) permanently destroy all such Personal Data and copies thereof and, in any event, certify in writing to Groups.io that it has done so. The Parties agree that Provider may retain one copy of the Personal Data as strictly necessary to comply with any legal, regulatory, judicial, audit or internal compliance requirements. Provider shall warrant that it will guarantee the confidentiality and security of the Personal Data and will not actively Process it anymore and destroy it as soon as legally allowed.

2.13. Audit. Upon request and without undue delay, Provider shall make available to Groups.io all information necessary to demonstrate (i) Provider's compliance with this DPA and (ii) Groups.io's compliance with its undertakings under applicable Data Protection Laws. Further, Groups.io, any third party appointed by it, bound by a duty of confidentiality, or a competent Supervisory Authority, shall be entitled to conduct an audit of Provider's (and/or any of its subcontractors) data Processing facilities and activities to ensure compliance with this DPA and the regulatory undertaking bearing upon Groups.io. Such audits shall be performed during normal business hours and in a way that does not interfere with normal business activities of Provider and, where relevant, Provider' subcontractors. Provider shall reasonably cooperate with the appointed auditor to conduct this audit. Should the audit show a breach to this DPA or to the Data Protection Laws, especially but not limited to security or

confidentiality requirements, Groups.io may require Provider to immediately remedy to this breach.

2.14.Subcontracting. Provider shall be allowed to engage subcontractors for carrying out specific Personal Data Processing activities, subject to the following: (i) Provider shall inform Groups.io in writing of any intended changes concerning the addition or replacement of subcontractors, thereby giving Groups.io the opportunity to object to such changes, (ii) Provider shall impose on its subcontractor(s), by way of a written agreement, the same and no less stringent obligations as are imposed on Provider under this DPA**;** (iii) Provider shall keep a list of all such subcontracting agreements, which list shall be made available to Groups.io upon request; (iv) Provider shall provide a copy of such subcontracting agreements to Groups.io (in which commercial information may be removed) upon request and acknowledges that Groups.io may share such copy with the relevant data protection supervisory authorities as necessary to comply with applicable law; and (iv) Provider shall, at no charge for Groups.io , actively monitor, regularly audit and, where applicable, take steps to enforce compliance of its subcontractors with their contractual obligations, reporting promptly to Groups.io any detected or reported non-compliance and all measures taken to remedy such non-compliance. If a subcontractor fails to remedy said non-compliance within a reasonable time after notice from Provider requiring remedy, Groups.io shall be entitled, without prejudice to any other right or remedy under Agreement, this DPA or applicable law, to require Provider to cease using the corresponding subcontractor and resume the provision of that part of the Services itself as per the Agreement. In any event, where a subcontractor fails to fulfil its data protection obligations under its written agreement with Provider, Provider shall remain fully liable to Groups.io for the performance of the subcontractor's obligations.

2.15.Data Transfers. Provider acknowledges that some Data Protection Laws may require additional measures be taken to secure transfers of Personal Data outside the country or region they originate from. In such a case, Provider shall assist Groups.io and, where relevant, Groups.io affiliates, in implementing these additional measures and, for instance, enter into separate Personal Data transfer agreements, where and as mandated under Data Protection Laws. Without limiting the generality of the foregoing, Provider shall refrain from transferring any Personal Data to a country which would not be deemed as offering an adequate level of protection by the European Commission, without relying, for the entire duration of the Agreement, on (i) an agreement strictly based on the European Commission Decision of 5 February 2010, as provided in Appendix 1 hereto, including any European Commission Decision updating or replacing the aforementioned Decision, entered into with Groups.io and/or Groups.io affiliates or, if agreed by Groups.io, (ii) an alternate mechanism in accordance with the applicable legislation of the European Union. In the event that any transfer mechanism under Data Protection Laws of the European Union is determined by the European Court of Justice or another organism of the European Union not to be adequate, Provider shall, as soon as possible, adopt and implement an appropriate alternative transfer mechanism. In the event that Provider fails to adopt an alternative transfer mechanism within one (1) month of the invalidation decision by the European Union organism, notwithstanding anything to the contrary in the Agreement, Groups.io may terminate the Agreement, at no cost, as of right and without prejudice to Groups.io's other rights and remedies. In any case, Groups.io and Provider agree that, in relation to transfer and Processing of any Personal Data, the provisions of the transfer mechanisms used (e.g., separate agreement(s)) will prevail over those of the Agreement and of this DPA in case of inconsistency.

3. Duration

1. This DPA shall come into force from its date of execution by both Parties, and shall remain into effect throughout the term of the Agreement. Notwithstanding the expiration or termination of the Agreement or this DPA, Section 2 of this DPA shall remain into effect provided that Provider still hold, store or otherwise Process Personal Data as part of the Agreement or this DPA.

4. Miscellaneous

Notwithstanding anything to the contrary in this DPA or in the Agreement, the liability of Provider for any breach of this DPA shall not be subject to the limitations of liability provisions included in the Agreement, if any.

Provider shall indemnify and hold Groups.io harmless against every claim, litigation, compensation or sanction, of any nature (civil, administrative or criminal), which would arise from the violation by the Provider of the commitments contained in this DPA. Where relevant, the Provider shall compensate Groups.io for any conviction and legal expenses, including reasonable attorney's fees, pronounced against Groups.io in a judicial or administrative decision which has become enforceable.

The Parties acknowledge and agree that the activities performed by Provider under this DPA do not involve any right to specific compensation other than that compensation owed to Groups.io for the provision of Services in accordance with the Agreement.

This DPA sets out the entire agreement and understanding between the Groups.io and Provider with respect to the Processing of Personal Data by Provider for the purpose of providing the Services and supersedes all other understandings or agreements made between Groups.io and Provider on the same subject matter. In case of conflict or inconsistency between the Agreement and this DPA, the provisions of this DPA shall prevail.

Except as mandated under applicable Data Protection Laws, any dispute relating to this DPA shall be governed by and interpreted in accordance with the law of the country and subject to the jurisdiction referred to in the Agreement.

IN WITNESS THEREOF, Groups.io and Provider have executed this DPA in *[Location TBC]* as of *[Date TBC]*.

Provider	Groups.io
By: _____	By: _____
Name: _____	Name: Mark Fletcher
Title: _____	Title: CEO
Date: _____	Date: _____

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA FROM THE COMMUNITY TO THIRD COUNTRIES (CONTROLLER TO PROCESSOR)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Clause 1 – Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 – Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 – Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has

assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 – Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorized access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 – Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 – Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 – Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 – Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 – Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 – Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 – Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/ or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 2
DESCRIPTION OF PROCESSING OPERATIONS

Data subjects

Customer may submit personal data to the Services, the extent of which is determined and controlled by Customer and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Authorized Users;
- employees of Customer;
- consultants of Customer;
- contractors of Customer;
- agents of Customer; and/or
- third parties with which Customer conducts business

Categories of data

The personal data transferred concert the following categories of data:

- Any personal data comprised in Customer Data, as defined in the Agreement.

Special categories of data (if appropriate)

Customer may submit personal data to Groups.io through the Services, the extent of which is determined and controlled by Customer in compliance with applicable Data Protection Law and which may concern the following special categories of data, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic or biometric data;
- health; and
- sex life.

Processing Operations

The personal data transferred will be processed in accordance with the Agreement and any Order Form and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain, and update the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement, as compelled by law.

APPENDIX 3

DESCRIPTION OF PROVIDER'S TECHNICAL AND ORGANIZATIONAL MEASURES

Control Category	Control Type	Control Description
Physical	Third Party Data Center	Physical access control lists manage ingress and egress Security fencing Biometric readers at all main entry points 24x7x365 security officers with fixed locations at front and rear access points 24x7x365 CCTV recordings Access control (mantraps)
Administrative	Policy	Security Account Password Handling of Personal Information Off Boarding Access Control
Administrative	Process	Incident response Patching
Administrative	Standards	Coding Security Standards for Managed Applications Server Build Data Retention and Disposal Key Management
Administrative	Compliance	Security Compliance Account Compliance
Administrative	Training	Security Awareness User Compliance Training
Technical	Preventative	Monthly Vulnerability Scans Malware Scans Firewall Anti-Virus IP Whitelisting & Blacklists
Technical	Detective	Infrastructure Access Logs Application Access Logs Application Audit Trails Application Login Logs
Technical	Access Control	Roles and Permissions VPN – Operational / Admin 2 factor auth on application
Technical	Encryption	SSL Data Encryption in Transit Data Encryption at Rest Password Encryption Use of strong encryption protocols such as AES

Control Category	Control Type	Control Description
Technical	User Controls	User Authentication Account Expiry Password Complexity Account Lockout Session Timeouts Application Whitelisting