DATA PROCESSING AGREEMENT

A. The Data Controller is appointing the Data Processor as its sub-contractor for the purpose of hosting solutions (the "**Service**").

B. Under the EU General Data Protection Regulation ("**GDPR**"), the Data Controller is required to implement an agreement between the Data Controller and any organisation which processes personal data on its behalf, governing the processing of that data.

C. The parties now wish to enter into this Agreement in order to regulate the provision and use of Personal Data which the Data Processor will be processing on behalf of the Data Controller.

D. If the Data Controller wishes to use the Data Processor's Service, the Data Controller accepts and agrees to be bound by and comply with this Agreement. Continued use of the Data Processor's Service indicates the Data Controller's continued acceptance of this Agreement. If the Data Controller does not agree with this Agreement, the Data Controller must not use Data Processor's Service.

AGREEMENT

1. DEFINITIONS AND INTERPRETATION

1.1 The following words and phrases used in this Agreement and the Schedules shall have the following meanings except where the context otherwise requires:

"Applicable Privacy Laws"	Refers to, where applicable, the Act Respecting the protection of personal information in the private sector - the "Quebec Act"; the Personal Information Protection and Electronic Documents Act – "PIPEDA"; the Personal Information Protection Act of British-Columbia – PIPA BC; the Personal Information Protection Act of Alberta – PIPA AB; the EU General Data Protection Regulation - the "GDPR", as well as any other applicable legislation, regulation, recommendation or opinion replacing, adding to or amending, extending, reconstituting or consolidating the

Applicable Privacy Laws.

“Data Controller”	Refers to the party who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
“Data Processor”	A person or entity who processes personal data on behalf of the Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, i.e. Meteor.
“Data Subject”	Refers to an individual who is the subject of personal data, i.e. to whom the data relates either directly or indirectly.
“Personal Data”	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller or Data Processor.
“Service”	Refers to the services by the Data Processor, notably the hosting solutions.
“GDPR”	Refers to the EU General Data Protection Regulation - the “GDPR”, as well as any other applicable legislation, regulation, recommendation or opinion replacing, adding to or amending, extending, reconstituting or consolidating the GDPR.

For the avoidance of doubt, all references to the "Agreement" shall include this DPA (including its appendices).

2. OBLIGATIONS OF THE DATA CONTROLLER

2.1 The Data Controller is responsible for determining, establishing and securing the legal basis, including with respect to the Data Subjects, for the processing of his or her Personal Information.

2.2 The Data Controller shall provide the Personal Data to the Data Processor together with such other information as the Data Processor may reasonably require in order for the Data Processor to provide the Service.

2.3 The instructions given by the Data Controller to the Data Processor in respect of

the Personal Data shall at all times be in accordance with all Applicable Privacy Laws and shall be in a written and duly documented form.

2.4 The Data Controller shall determine the retention period of Personal Information in relation to the purposes for which they were collected and in accordance with the Applicable Privacy Laws.

3. OBLIGATIONS OF THE DATA PROCESSOR

3.1 The Data Processor undertakes that it shall process the Personal Data strictly in accordance with the Data Controller's written and duly documented instructions for the processing of that Personal Data. If the Data Processor acts outside the Data Controller's instructions or contrary to these instructions, the Data Processor will be considered as Data Controller within the meaning of the GDPR and will assume all liabilities and consequences, in particular financial liabilities and consequences.

3.2 If the Data Processor considers that an instruction from the Data Controller constitutes a violation of the GDPR, it shall inform the Data Controller as soon as possible.

3.3 The Data Processor will process the Personal Data only for the purposes of the performance of the Service, *i.e*. to provide a hosting solution.

3.4 The Data Processor will ensure, as far as possible, that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data. The Data Processor will ensure that all such employees have undergone training in the law of data protection, their duty of confidentiality under contract and in the care and handling of the Personal Data.

3.5 The Data Processor will make its best efforts to assist the Data Controller with all individuals' requests which may be received from Data Subjects to whom the Personal Data refers.

3.6 The Data Processor will make its best efforts to collaborate with the Data Controller, in particular by providing it with the necessary documentation to demonstrate compliance with all its obligations, in particular the performance of audits, including inspections, by the Data Controller or another auditor (that is independent and not a competitor of the Data Processor) that the Data Controller has mandated, and contribute to such audits.

3.7 The Data Processor will not disclose the Personal Data to a third party in any

circumstances other than at the specific written request of the Data Controller, unless the disclosure is required by law.

3.8 The Data Controller recognizes and agrees that the Processor may store the Personal Data, in its possession, outside the European Economic Area (EEA) or the United Kingdom to a third country recognized by an adequacy decision of the European Commission, as providing an adequate level of protection for Personal Data, and, in any case, with appropriate safeguards, notably in the United States, approved by the EU authorities under EU data protection laws, including the GDPR, and set out in Annex 4 (the “Standard Contractual Clauses”). For the sake of clarity, the Data Processor will comply with the obligations of the ‘data importer’ in the Standard Contractual Clauses and the Data Controller will comply with the obligations of the 'data exporter'.

3.9 The Data Processor will not sub-contract any of the processing without the prior general consent of the Data Controller, it being specified that the Data Processor shall ensure that all of the Data Processor’s obligations under the Agreement are respected by any company replacing the Data Processor and any subcontractor, regardless of its rank or method of intervention, by expressly providing for these same obligations in the contract binding the Data Processor to the said company or the subcontractor to any subsequent subcontractor, so that they undertake to respect the Agreement. The Data Processor shall make available to the Data Controller a list of Sub-Processors authorized to Process Personal Information and provide the Data Controller with a mechanism to obtain notice of any updates to such list. Notification of a new Sub-Processor shall be issued prior to such new Sub-Processor being authorised to Process Personal Information in connection with the DPA. At the time of the signature of this DPA, the Data Controller has agreed to the sub-contractors listed in the Appendix 3 of this DPA. If the Data Controller objects to Data Processor’s use of a new Sub-Processor, the Data Controller shall notify the Data Controller promptly in writing within ten (10) days after notification regarding such Sub-Processor. If the Data Controller objects to the use of a third party or refuses to grant permission for the use of a third party by the Data Processor, the Data Processor shall suggest another third party. If it is not possible, and insofar as the refusal reasonably justifies this according to Data Processor, the Data Processor has the right to terminate the DPA without being liable to pay any damages to the Data Controller. In this case, the Data Processor will apply a notice period of 1 month. At the time of this agreement, the Data Controller has agreed to the sub-contractors listed in the Annex 3 of this Agreement. The Data Processor shall be liable for the acts and omissions of any Sub-Processors to the same extent as if the acts or omissions were performed by the Data Processor.

3.10 The Data Processor will make its best efforts to use appropriate operational and technological processes and procedures to guarantee the security of its premises

and to keep the Personal Data safe from unauthorized use or access, loss, destruction, theft, alteration, distortion, disclosure or any other modification.

3.11 The Data Processor will inform, without undue delay, the Data Controller in case of a request from an administrative or judiciary authority received by the Data Processor related to the Processing of Personal Data made in respect of Services.

3.12 The Data Processor will not store Personal Data beyond the retention period fixed by the Data Controller in relation to the purposes for which they were collected and, in any event, not to store them after the expiration of the Agreement, except in the event of any legislative or regulatory provision or any administrative or judicial decision stating the contrary.

3.13 The Data Processor will notify the Data Controller of any information security incident that may impact the processing of the personal data covered by this agreement without undue delay after discovering, or becoming aware of any such incident. The Data Processor will make its best efforts to co-operate with the Data Controller in implementing any required corrective action agreed between the parties.

3.14 The Data Controller reserves the right subject to at least one month's written notice prior to the date of the audit and within normal business hours to carry out compliance and information security audits of the Data Processor, in order to satisfy itself that the Data Processor is adhering to the terms of this agreement. Where a sub-contractor is used, the Data Processor agrees that the Data Controller may also, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks of the sub- contractor to ensure adherence to the terms of this Agreement.

3.15 At the termination of the Agreement, the Data Processor will delete or return all the Personal Data to the Data Controller at the Data Controller’s choice, and delete existing copies unless European Union or Member State law requires storage of the Personal Data.

4. THIRD PARTY RIGHTS

The Data Subject is hereby entitled to enforce the terms and conditions of this Agreement as a third party beneficiary.

5. INDEMNITIES

Each party shall indemnify the other against all costs, expense, including legal expenses, damages, loss, including loss of business or loss of profits, liabilities, demands, claims, actions or proceedings which a party may incur arising out of any breach of this Agreement howsoever arising for which the other party may be liable.

6. GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the applicable laws of Canada and, where applicable, with the GDPR and each party hereby submits to the non-exclusive jurisdiction of the appropriate courts.

ANNEX 1
PROCESSING OF PERSONAL DATA

PERSONAL DATA AND PURPOSES

Controller tasks Processor with the processing of the following Personal Data:

−Username, email, billing information

The activities for which abovementioned Personal Data may be processed are:

−The provision of hosting solutions

ACCESS

Processor will store and process all Personal Data strictly separated from personal data that it processes on its own behalf or on behalf of third parties.

Only the following groups of people will have access to the Personal Data:

- The system developer, account manager, support service engineer, administrators, IT experts of the Sub-processor engaged by Processor, exclusively on a ‘need-to-know’ base to support the technical operation and hosting and, if necessary, development of the application;

DURATION

The Personal Data Processed by Processor will be Processed for the following duration:

−While the Data Controller keep using the Data Processor services

DATA SUBJECTS

The Personal Data Processed by Data Processor concern the following categories of Data Subjects:

−the creation of an user to access and use our services
−segmented marketing messages and transactional messages

ANNEX 2
SECURITY MEASURES

The security measures taken by the Data Processor:

Description of the technical and organizational security measures implemented by the Data Processor

As specified in the Data Processing Agreement, the Data Processor shall take technical and organizational measures – taking into account the state of the art and the costs of implementing these measures – to protect Personal Data against loss, unlawful processing or unlawful access. The measures taken are listen in this appendix and are supplemented or amended if necessary.

Platform Architecture
Meteor Cloud's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology.

Meteor Cloud consists of Platform services built and run on top of Amazon's Elastic Container Service and Amazon Web Services.

Meteor Cloud utilizes Amazon EC2 virtual machine and Docker isolation mechanisms. Each application instance is run in its own Docker container on an Amazon EC2 virtual machine.

Risk Assessment
Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Amazon's data center operations have been accredited under:
ISO 27001
SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) PCI Level 1
FISMA Moderate
Sarbanes-Oxley (SOX)
Meteor Cloud itself has not pursued independent certifications.

Policy around Software Security Updates
System configuration and consistency is maintained through standard images, configuration management software, and the replacement of select systems with updated deployments.

Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

Customer Data Security
Customer application configuration secrets are stored in a Meteor Cloud system database. This database is secured by standard system and authorization policies. Access to the database is restricted to authorized personnel only, for purposes of administration and support.

Customer application certificates and keys are stored in encrypted form in the Meteor Cloud system database. These certificates are only decrypted on the Meteor Cloud Proxy machines, and are not exposed to application containers.

Access to private information is protected using Docker isolation in the application container.

Application Data
Meteor Cloud provides SSL encryption to protect data transmission over the wire from external entities to the Meteor Cloud Proxy layer. Internally in Meteor Cloud, Amazon EC2 virtual machine and Docker container network isolation is utilized to protect data transmission over the wire.

Meteor Cloud does not maintain databases that are utilized for production application use. These databases are provisioned, configured and maintained by the customer.

Meteor Cloud offers free shared database clusters only for hobby and demo projects, these projects shouldn't store customers' data.

Application Logs

Meteor Cloud captures and stores Application Logs in an off-site database. This database is secured by standard system and authorization policies. Access to the database is restricted to authorized personnel for the purposes of administration and support only.

Operational Policies

Meteor Cloud employees do not access customer data or customer environments as part of day-to-day operations. When customers need support, authorized employees are able to view customer data when specifically requested.

All company employees are trained to understand that customer data privacy and confidentiality is paramount. Under no circumstances is customer data ever disclosed to a third-party. Only a limited subset of employees have the ability to view customer environments and stored data.

Access is routinely evaluated to ensure those rights are retained only when necessary by job function. Meteor Cloud maintains a policy and operational checklist for removing access for employees that are no longer associated with its operations.

ANNEX 3
SUB-PROCESSORS

The following Sub-processors have already been engaged by the Data Processor at the time of the conclusion of the Data Processing Agreement.

Controller has given permission for the engagement of these Sub-processors.

Name of the Sub-processors	**Activity of the Sub-processor**	**Location of the Sub-processor**	**Appropriate Safeguards for the transfer of Personal Data**
Recurly	Payment gateway	USA (San Francisco, California)	Standard Contractual Clauses
Mailchimp	Newsletter	USA (Atlanta, Georgia)	Standard Contractual Clauses
AWS	Cloud computing	USA (Seattle, Washington)	Standard Contractual Clauses
MongoDB Atlas	DB hosting	USA (New York, New York)	Standard Contractual Clauses
Scalegrid	DB hosting	USA (Palo Alto, California)	Standard Contractual Clauses

ANNEX 4

STANDARD CONTRACTUAL CLAUSES

Document attached.