LEGAL

Data Processing Agreement

Effective Date: September 6, 2026 · Version 1.0

This Data Processing Agreement (the "DPA", version 1.0) forms part of the Terms of Service and applies to every organizer whose use of Lime-n.io involves personal data of people in the European Union or the European Economic Area, Switzerland, the United Kingdom or Quebec. Its body is the standard contractual clauses between controllers and processors adopted by the European Commission in **Commission Implementing Decision (EU) 2021/915** of 4 June 2021, reproduced without modification, together with the Annexes below. Annexes I to IV are the Annexes the Clauses call for. Annex V and Annex VI are additional annexes agreed under Clause 2(b); they add safeguards and do not contradict the Clauses.

No signature is needed: accepting the Terms of Service accepts this DPA. If your organization needs a countersigned copy, write to privacy@lime-n.io and we will return one.

The Parties

The controller is the organizer identified by the account that accepted the Terms of Service — the name, organization and contact details held in that account.

The processor is Harvest Technology Systems, Inc., trading as Lime-n.io, of 78 Parkhaven Drive, St. Jacobs, ON, Canada N0B 2N0. Contact: Stu Doherty, privacy@lime-n.io.

The Parties are the controller and the processor. Full details are in Annex I.

Standard contractual clauses

Section I

Clause 1 — Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 — Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 — Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 — Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 — Optional: Docking clause

The optional docking clause is not used. Clause 5 of the Decision is left unadopted, and the numbering of the remaining Clauses is unchanged.

Section II — Obligations of the Parties

Clause 6 — Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 — Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (“sensitive data”), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including

personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 — Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the

processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
4. the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 — Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the likely consequences of the personal data breach;
3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III — Final provisions

Clause 10 — Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
2. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Annex I — List of parties

Controller

- Name: the organizer named on the account that accepted the Terms of Service.
- Address: the organization address held in that account.
- Contact person's name, position and contact details: the account owner, as held in that account.
- Signature and accession date: by accepting the Terms of Service, on the date of acceptance recorded on the account.
- The controller's data protection officer, if any, as notified to privacy@lime-n.io.

Processor

- Name: Harvest Technology Systems, Inc., trading as Lime-n.io.
- Address: 78 Parkhaven Drive, St. Jacobs, ON, Canada N0B 2N0.
- Contact person's name, position and contact details: Stu Doherty, person responsible for personal information, privacy@lime-n.io.
- Signature and accession date: signed as set out under "Signatures" below, effective on the date stated at the head of this document.
- No data protection officer is appointed; the processor is not required to appoint one, and the person named above answers every request.

Annex II — Description of the processing

Categories of data subjects whose personal data is processed. Guests who register for the controller's events, and the people in their party where the guest names them; the controller's own team — promoters, sub-promoters and door staff — and the controller's account holders.

Categories of personal data processed. For guests: name, email address, phone number where given, size of party, registration status and time, arrival status and time, and the promoter who registered them. For team members and account holders: name, email address, phone number where given, role, organization membership, sign-in identifiers and the times of their actions in the service.

Sensitive data processed. None. The service neither asks for nor is intended to receive data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences. The controller instructs the processor not to enter such data into the service.

Nature of the processing. Collection of guest registrations through invitation links; storage; organisation of those registrations into event guest lists; making the lists available to the controller's team according to role; recording arrivals at the door; producing counts and statistics for the controller; sending transactional email to guests and team members; making the data available to the controller as an export; and erasure.

Purpose(s) for which the personal data is processed on behalf of the controller. Solely to provide the guest-list service to the controller: to build and manage guest lists for the controller's events, to admit guests at the door, to inform guests and team members about the events they are on, to give the controller counts and totals for its own events, and to return the controller's data to it on request. The processor does not use the data for its own purposes, does not sell personal data, and does not share it for advertising.

Duration of the processing. For the life of the controller's account, subject to these retention periods, which the processor applies without being asked:

- Guest data is deleted 90 days after the date of the event it belongs to, by a process that runs every day.
- Account and organization data is deleted within 180 days of the account ending.
- A request from the controller to delete a guest, a team member or the whole organization is actioned within 14 days.
- Backups are retained 7 days, after which deleted data is gone from them too.

For processing by sub-processors, subject matter, nature and duration. As set out for each sub-processor in Annex IV. Each sub-processor processes only for the purpose stated there, for no longer than the processor itself retains the data.

Competent supervisory authority. The supervisory authority of the controller's place of establishment, or of the Member State where the data subjects concerned are located, as Regulation (EU) 2016/679 provides. For Switzerland, the United Kingdom and Quebec, see Annex VI.

Annex III — Technical and organisational measures

Measures implemented by the processor to ensure an appropriate level of security, described concretely:

- **Protection of data during transmission.** All traffic between the browser, the service and its providers is encrypted with TLS; the service is served over HTTPS only.
- **Protection of data during storage.** All stored data is encrypted at rest by the infrastructure provider named in Annex IV.
- **User identification and authorisation.** Every read and every write is checked, at the point of access, against the identity of the person making it and the membership that person holds in the controller's organization: everyone on the controller's team who has an account — owners, admins, promoters and door staff — can see the details of guests on that organization's events, and no one who has not been given access by the organizer can; anonymous visitors to an invitation link are described under Data minimisation below. Guests are told on the sign-up form that the promoter who invited them and their team can see their details.
- **Events logging.** An activity trail records who did what and when; it can be written only by the processor's own trusted code and never by a signed-in person.
- **Ability to restore availability.** Backups are taken daily and retained 7 days, so data can be restored after a technical incident.
- **Data minimisation.** A page opened from an invitation link without signing in shows the list stripped of email addresses and phone numbers.
- **Limited data retention.** Guest data is deleted 90 days after the event automatically, on a schedule that runs daily; the other periods in Annex II apply likewise.

- **Ongoing confidentiality.** Error reports collected to fix faults carry technical context only, never names, email addresses or guest data.
- **Confidentiality of personnel.** Access to the controller's data is limited to those of the processor's staff who need it to run the service — today, one person, the individual named in Annex I — bound to confidentiality.
- **Accountability.** The processor keeps and follows a written runbook for data subject requests and a written runbook for security incidents; the record of processing activities is maintained and available to a supervisory authority on request.

Assistance to the controller (Clause 8(d)). The processor gives the controller the means to answer a data subject itself: an export of any event's guest list, on demand from the event page. Where an export is not enough, the processor answers a written request to privacy@lime-n.io within 14 days, and carries out a deletion in the same period. The processor notifies the controller of any request a data subject sends it directly and does not answer it itself unless the controller so instructs or cannot be reached.

Elements of a breach notification (Clause 9.2). The processor notifies the controller by email to the account owner within 48 hours of becoming aware of a personal data breach affecting the controller's data, and includes what Clause 9.2 (a) to (c) requires along with the events and organizations affected, the period covered, and the steps taken — enough for the controller to make its own notification.

Audits under Clause 7.6. The controller gives at least 30 days' written notice, audits at most once in any 12 months unless a personal data breach or a supervisory authority requires otherwise, bears its own costs, and accepts a written report or documentation where that reasonably answers the question.

Measures not claimed. The processor holds no SOC 2 or ISO 27001 certification, runs no external penetration test programme, and has not appointed a data protection officer. It states this rather than leave it to be assumed.

Annex IV — List of sub-processors

The controller has authorised the use of the following sub-processors. The processor informs the account owner by email at least 30 days before adding or replacing one. The controller may object by reply; if the objection cannot be resolved, the controller

may terminate the affected part of the service and export its data before the change takes effect.

Sub-processor	Description of the processing	Categories of data	Location	Transfer basis
Google Cloud / Firebase Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA, USA	Hosting, stored data, processing, sign-in, and (after consent) product analytics	All account and guest data held by the service	United States (nam5 multi-region storage; us-east4 processing)	Google Cloud Data Processing Addendum with EU Standard Contractual Clauses; Google LLC is certified under the EU-US Data Privacy Framework and its UK and Swiss extensions
Resend Resend, Inc., USA	Delivery of transactional email (confirmations, invitations, reminders, recaps, billing notices)	Recipient name and email address, event and organization details in the message	United States	Resend Data Processing Agreement with EU Standard Contractual Clauses
Stripe Stripe, Inc., USA (and Stripe Payments Company)	Subscription billing for organizer accounts; card details are collected and held by Stripe only	Billing name, email, subscription status	United States	Stripe Data Processing Agreement with EU Standard Contractual Clauses; Stripe is certified under the EU-US Data Privacy Framework
Sentry Functional Software, Inc. (Sentry), USA	Error reports from the app and its services, so faults can be fixed	Technical error context only; no names, email addresses or guest data by design	United States	Sentry Data Processing Addendum with EU Standard Contractual Clauses; Sentry is certified under the EU-US Data Privacy Framework

Responsibilities are delimited as follows: the infrastructure provider holds all of the data; the email provider receives only the recipient and the content of each message sent; the billing provider receives only the organizer's billing details and never guest data; the error-reporting provider receives technical context only.

Annex V — International transfers

Where the data is. All data is held on Google Cloud in the United States: stored in the nam5 (US multi-region) and processed in us-east4. The processor itself is established in Ontario, Canada. Personal data is transferred to no other country than those named in this Annex.

The chain, in order:

1. **Controller (EU/EEA, United Kingdom, Switzerland or Quebec) to the processor in Canada.** Canada benefits from an adequacy decision of the European Commission for personal data transferred to recipients subject to the Personal Information Protection and Electronic Documents Act (Decision 2002/2/EC, maintained following the Commission's 2024 review of adequacy decisions adopted under Directive 95/46/EC). The United Kingdom maintains equivalent adequacy regulations for Canada, and Canada appears on the list of states with adequate protection published by the Swiss Federal Council. No further transfer tool is required for this leg.
2. **Processor to Google LLC (United States).** The Google Cloud Data Processing Addendum applies, incorporating the standard contractual clauses adopted by the Commission in Implementing Decision (EU) 2021/914 for transfers to third countries. Google LLC is certified under the EU-US Data Privacy Framework and its UK and Swiss extensions.
3. **Processor to Stripe and to Sentry (United States).** Each of them is certified under the EU-US Data Privacy Framework and is additionally bound by the standard contractual clauses in its own data processing agreement.
4. **Processor to Resend (United States).** Bound by the standard contractual clauses in its data processing agreement.

The current text of each provider's agreement is linked from Annex IV and from the trust page.

Annex VI — Regime addenda

European Union and European Economic Area

Regulation (EU) 2016/679 governs, and the Clauses apply as written. The processor has not appointed a representative under Article 27. It considers the exemption in Article 27(2)(a) to apply at its current scale and reviews that assessment on taking on each customer established in the Union.

Switzerland

References in the Clauses to Regulation (EU) 2016/679 are read as references to the Swiss Federal Act on Data Protection of 25 September 2020, in force since 1 September 2023, and to its Ordinance. The competent authority is the Federal Data Protection and Information Commissioner. Canada appears on the Federal Council's list of states providing adequate protection. References to a Member State are read as references to Switzerland, and the Clauses also protect data relating to legal entities to the extent Swiss law requires.

United Kingdom

References in the Clauses to Regulation (EU) 2016/679 are read as references to the UK GDPR and the Data Protection Act 2018, and references to a Member State are read as references to the United Kingdom. The competent authority is the Information Commissioner's Office. Canada is covered by the United Kingdom's adequacy regulations. The processor has not appointed a representative under Article 27. It considers the exemption in Article 27(2)(a) to apply at its current scale and reviews that assessment on taking on each customer established in the United Kingdom.

Quebec

This DPA is the written agreement required of a service provider by section 18.3 of the Act respecting the protection of personal information in the private sector. Under it the processor: uses the personal information only for the purposes of the service set out in Annex II; keeps it confidential; does not keep it after the end of the service, deleting it as set out in Annex II; notifies the controller of any confidentiality incident concerning that information within 48 hours of becoming aware of it; and allows the controller to verify that these obligations are met, on the terms in Annex III.

The person responsible for the protection of personal information at the processor is Stu Doherty, privacy@lime-n.io. The controller's assessment of the transfer outside

Quebec required by section 17 is supported by the fact sheet at /trust/quebec, which the processor keeps current. The competent authority is the Commission d'accès à l'information du Québec.

Liability and precedence

Liability under these Clauses is subject to the limitation in section 9 of the Terms of Service to the extent the Clauses permit; nothing here creates an indemnity beyond the Clauses.

If these Clauses conflict with the Terms of Service, the Clauses prevail for the processing they govern.

Signatures

For the processor. Signed by Stu Doherty for Harvest Technology Systems, Inc. on the effective date stated at the head of this document.

Signature — Stu Doherty, Harvest Technology Systems, Inc.

For the controller. By accepting the Terms of Service. A countersignature is not required; where your organization needs one, sign below and return the document to privacy@lime-n.io.

Signature — name, position, organization, date