Legal

Data Processing Agreement

Version 1.1, effective November 18, 2026 Questions: privacy@northdue.com

1. Scope and parties

This Data Processing Agreement ("DPA") is between Riverstone Ventures F LLC, a Minnesota limited liability company, 2411 121st Cir NE, Unit J, Blaine, MN 55449-5592, United States ("Northdue"), and the business that has agreed to Northdue's Terms of Service or signed an order form with Northdue ("Client"). It forms part of that agreement (the "Agreement") and applies whenever Northdue processes Client Personal Data while providing the Northdue service (the "Service"). It takes effect when the Client accepts the Agreement, and no separate signature is needed. A Client that wants a countersigned copy can ask at privacy@northdue.com.

2. Definitions

- **Data Protection Laws** means all laws on privacy and the processing of personal data that apply to a party's processing under the Agreement, including, where they apply, the EU General Data Protection Regulation 2016/679 ("GDPR"), the GDPR as it forms part of UK law ("UK GDPR") and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection ("FADP"), and US state laws such as the California Consumer Privacy Act as amended ("CCPA").
- **Client Personal Data** means personal data that Northdue processes on the Client's behalf in providing the Service, as described in Annex 1.
- **Controller**, **processor**, **data subject**, **personal data**, **processing** and **supervisory authority** have the meanings given in the GDPR. **Business**, **service provider**, **sell** and **share** have the meanings given in the CCPA.
- **Subprocessor** means a third party Northdue engages to process Client Personal Data.
- **Security Incident** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data.
- **SCCs** means the standard contractual clauses approved by the European Commission in Implementing Decision (EU) 2021/914. The **UK Addendum** means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner.

3. Roles

For Client Personal Data, the Client is the controller (or a processor acting for its own controller) and Northdue is the Client's processor and service provider. Each party will comply with the Data Protection Laws that apply to it. The Client is responsible for having a lawful basis for the processing it instructs, for

the accuracy of the data it provides, and for giving any notices the law requires to the people whose data it provides.

Northdue is a separate controller for personal data it processes for its own business, such as its clients' account and billing information and website inquiries, as described in its Privacy Policy.

4. Processing on instructions

- Northdue will process Client Personal Data only on the Client's documented instructions. The Agreement, this DPA, and the Client's use and configuration of the Service are the Client's complete instructions. Further instructions must be in writing and consistent with the Agreement.
- Northdue may also process Client Personal Data where the law requires it. In that case it will tell the Client first, unless the law forbids it.
- Northdue will tell the Client if, in its opinion, an instruction breaks Data Protection Laws.
- Northdue will not use Client Personal Data to train artificial intelligence models, and will not allow its Subprocessors to do so.

5. Confidentiality of personnel

Northdue will ensure that anyone it authorizes to process Client Personal Data is bound by confidentiality obligations and accesses it only as needed to provide, support and secure the Service, or as the law requires. Northdue staff don't read the Client's customers' emails or approve anything sent in the Client's name.

6. Security

Northdue will implement and maintain appropriate technical and organizational measures to protect Client Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, and the risks to individuals. The measures in place at the date of this DPA are described in Annex 2. Northdue may update them, as long as the overall level of protection doesn't decrease.

7. Subprocessors

- The Client gives Northdue general authorization to engage Subprocessors. The current Subprocessors are listed in Annex 3 and on Northdue's Subprocessors page.
- Northdue will tell the Client, by email to its account owner, at least 30 days before a new Subprocessor starts processing Client Personal Data. The Client may object on reasonable data protection grounds within that period. The parties will then discuss the objection in good faith. If they can't resolve it, the Client may cancel the affected Service before the change takes effect, without penalty.

- Northdue will bind each Subprocessor by a written agreement with data protection obligations no less protective than this DPA, and remains responsible to the Client for its Subprocessors' performance of those obligations.

8. Data subject requests

Taking into account the nature of the processing, Northdue will assist the Client by appropriate technical and organizational measures, as far as possible, to respond to requests from individuals to exercise their rights under Data Protection Laws. If Northdue receives such a request directly about Client Personal Data, it will pass it to the Client without undue delay and won't respond to it itself, except to say it has been passed on, unless the Client authorizes it to.

9. Security incidents

Northdue will notify the Client without undue delay, and where feasible within 72 hours, after becoming aware of a Security Incident affecting Client Personal Data. The notice will describe, as far as then known, the nature of the incident, the data and individuals affected, its likely consequences, and the measures taken or proposed. Northdue will take reasonable steps to contain and remedy the incident, provide further information as it becomes available, and give the Client reasonable help to meet its own notification obligations. Notifying the Client isn't an admission of fault.

10. Impact assessments and consultations

Northdue will give the Client reasonable information and help, taking into account the nature of the processing and the information available to it, for any data protection impact assessment or prior consultation with a supervisory authority that the Client is required to carry out about the Service.

11. Return and deletion

When the Service ends, the Client may export its data or ask for a copy. Northdue will delete Client Personal Data within 30 days after the end of the Service, or sooner at the Client's written request, unless the law requires it to keep some of it. Copies in backups are overwritten in the normal backup cycle, and until then remain protected under this DPA and aren't actively processed. Northdue will confirm deletion on request.

12. Audits

Northdue will make available to the Client the information reasonably needed to show compliance with this DPA, including its security documentation and, when available, third-party audit reports. If that information isn't enough to meet a requirement of Data Protection Laws or a supervisory authority, the Client may audit Northdue's compliance no more than once a year, on at least 30 days' written notice, during business hours, at the Client's cost, in a way that doesn't disrupt the Service or breach other clients' confidentiality, and subject to reasonable confidentiality terms. An auditor must not be a competitor of Northdue.

13. International transfers

Northdue and its Subprocessors process Client Personal Data in the United States. Where Client Personal Data subject to the GDPR, UK GDPR or FADP is transferred to Northdue in a country without an adequacy decision, the parties agree that:

- **EEA transfers** are governed by the SCCs, which are incorporated into this DPA by reference: Module Two (controller to processor) where the Client is a controller, and Module Three (processor to processor) where the Client is a processor. The Client is the data exporter and Northdue is the data importer. Clause 7 (docking) applies. Under Clause 9(a), Option 2 (general written authorization) applies, with the notice period in section 7 of this DPA. The optional wording in Clause 11 doesn't apply. Under Clause 13, the competent supervisory authority is the one that applies to the Client. Under Clauses 17 and 18, the SCCs are governed by the laws of Ireland and disputes go to the courts of Ireland. Annexes I and II of the SCCs are completed by Annexes 1 and 2 of this DPA, and the list of Subprocessors is in Annex 3.
- **UK transfers** are governed by the SCCs as varied by the UK Addendum. Table 1 is completed with the parties' details in this DPA, Tables 2 and 3 with the choices and annexes above, and in Table 4 either party may end the UK Addendum as its Section 19 allows.
- **Swiss transfers** are governed by the SCCs as adjusted for the FADP: references to the GDPR include the FADP, the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for those transfers, and the term "member state" doesn't prevent data subjects in Switzerland from bringing claims where they habitually reside.
- If a transfer mechanism is replaced or found invalid, the parties will cooperate to put in place an alternative that the law recognizes.

14. US state privacy laws

Where the CCPA or a similar US state law applies, Northdue acts as the Client's service provider or processor, and:

- won't sell or share Client Personal Data;
- won't retain, use or disclose it for any purpose other than the business purposes set out in the Agreement, including any commercial purpose other than providing the Service, or outside the direct business relationship between the parties;
- won't combine it with personal data it receives from or on behalf of anyone else, except as Data Protection Laws allow;
- will comply with the obligations that apply to it, provide the same level of privacy protection those laws require, and tell the Client if it can no longer meet them;
- gives the Client the right to take reasonable and appropriate steps to stop and remedy any unauthorized use of Client Personal Data.

15. General

- **Order of precedence.** If there's a conflict, the SCCs (where they apply) prevail over this DPA, and this DPA prevails over the rest of the Agreement as far as the processing of Client Personal Data is concerned.
- **Liability.** Each party's liability under this DPA is subject to the limitations in the Agreement, except where Data Protection Laws or the SCCs don't allow it to be limited.
- **Term.** This DPA lasts as long as Northdue processes Client Personal Data.
- **Changes.** Northdue may update this DPA to reflect changes in Data Protection Laws, its Subprocessors or the Service, as long as the changes don't reduce the protection of Client Personal Data. Northdue will publish the updated version here with a new date and tell clients about significant changes.
- **Governing law.** Apart from the SCCs, this DPA is governed by the law that governs the Agreement.

Annex 1: Details of the processing

Data exporter	The Client, as named in its Northdue account or order form. Role: controller (or processor). Contact: the Client's account owner.
Data importer	Riverstone Ventures F LLC, 2411 121st Cir NE, Unit J, Blaine, MN 55449-5592, United States. Role: processor. Contact: privacy@northdue.com.
Subject matter and purpose	Providing the Service: reading the Client's accounting data; deciding which of the Client's customers to follow up; drafting payment reminder emails for the Client's team to approve; sending approved emails from the Client's mailbox; reading and classifying replies and customer page answers; matching payments; producing reports; and supporting and securing the Service.
Nature of the processing	Receipt through connected accounts and uploads, storage, organization, retrieval, analysis (including with AI), transmission of approved emails, and deletion.
Categories of data subjects	The Client's users of the Service; the Client's business customers' employees and contacts; other senders whose messages to the Client's connected mailbox mention an invoice or payment.

Categories of personal data	Names, business email addresses, phone numbers and job titles; invoice, payment and balance information linked to those contacts; the content of emails and customer page answers about invoices or payments; notes the Client's team enters; and user account and activity records.
Sensitive data	None intended. The Client agrees not to provide special categories of personal data through the Service.
Frequency	Continuous, for as long as the Client uses the Service.
Duration and retention	For the term of the Agreement and then as set out in section 11 and the Privacy Policy.
Transfers to Subprocessors	As set out in Annex 3, for the purposes listed there and for the duration of the Agreement.

Annex 2: Technical and organizational security measures

- **Encryption in transit:** HTTPS for every page and connection, with HTTP Strict Transport Security.
- **Encryption at rest:** data and its automatic disk snapshots are stored on encrypted disks.
- **Connection tokens:** sign-in tokens for clients' accounting software and mailboxes are encrypted a second time (AES with an HMAC signature) with a key kept apart from the data.
- **Least access:** connections request the narrowest permissions the Service needs, and accounting connections are read-only.
- **Separation:** each client's records are kept apart, and client users can see only their own company.
- **Authentication:** passwords stored only as salted hashes; lockout after repeated failed sign-ins; two-step sign-in available to all users and enforceable by the client; sessions that expire and end when credentials change.
- **Application security:** anti-forgery tokens on every form, strict browser security headers, and automated tests of security controls.
- **Accountability:** an audit log of approvals, edits, rejections and setting changes, with the person's name.
- **Data minimization:** only the text needed to draft an email or read a reply is sent to the AI provider, which doesn't train on it under its commercial terms. Mailbox messages that aren't relevant aren't stored.
- **Backups and availability:** nightly backups, kept for seven days by default, with connection tokens still encrypted inside them.

- **Vendors:** Subprocessors are chosen for their security practices and bound by written data protection terms.
- **Vulnerabilities:** a public process for reporting security problems, at northdue.com/security.

Annex 3: Subprocessors

Subprocessor	Purpose	Location
Render Services, Inc. (Render)	Cloud hosting: runs the Northdue app and stores its data and backups	United States (Virginia)
Anthropic, PBC (Anthropic)	AI: drafts emails and understands customers' replies	United States
Stripe, Inc. (Stripe)	Billing and payments for Northdue's own subscription fees	United States
Google LLC (Google Workspace)	Northdue's own email: support, billing and account emails	United States

The current list is always at northdue.com/subprocessors.