NOUS · LEGAL

Data Processing Agreement

OpenNous LLC · Version dated 22 July 2026. This Data Processing Agreement forms part of the Agreement between the parties for the provision of the Nous service.

This Data Processing Agreement ("DPA") is entered into by and between OpenNous LLC ("Processor", "Nous", "we"), and the customer identified in the applicable order form or agreement ("Controller", "Customer", "you"). This DPA is incorporated into and governed by the terms of the master agreement or terms of service between the parties (the "Agreement"). It takes effect on the date the Agreement is signed or the Service is first used, whichever is earlier.

1. Definitions

Terms such as "Personal Data", "Processing", "Data Subject", "Controller", "Processor", and "Personal Data Breach" have the meanings given to them in applicable data protection law, including the EU General Data Protection Regulation 2016/679 ("GDPR") and the UK GDPR. "Applicable Data Protection Law" means all laws relating to data protection and privacy that apply to the Processing of Personal Data under the Agreement. "Subprocessor" means any third party engaged by the Processor to Process Personal Data.

2. Roles and scope of processing

The parties acknowledge that, for the Personal Data processed through the Service, the Customer is the Controller and Nous is the Processor. Nous will Process Personal Data only on the documented instructions of the Customer, including as set out in this DPA and the Agreement, and as necessary to provide and support the Service. The subject matter, duration, nature, and purpose of the Processing, and the categories of Data Subjects and Personal Data, are described in Annex I.

3. Customer instructions and compliance

Nous will Process Personal Data in accordance with the Customer's instructions and will inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. The Customer is responsible for the accuracy and legality of the Personal Data it connects to the Service and for having a valid legal basis for the Processing.

4. Confidentiality

Nous will ensure that personnel authorized to Process Personal Data are bound by appropriate confidentiality obligations and are granted access only on a need to know basis.

5. Security measures

Nous will implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. A description of these measures is set out in Annex II. Nous may update its measures over time provided the level of protection is not reduced.

6. Subprocessors

The Customer provides general authorization for Nous to engage Subprocessors to Process Personal Data. A current list of Subprocessors is maintained and made available to the Customer. Nous will impose data protection obligations on each Subprocessor that are no less protective than those in this DPA, and remains responsible for the performance of each Subprocessor. Nous will give the Customer notice of any intended addition or replacement of a Subprocessor and a reasonable opportunity to object on legitimate grounds.

7. Assistance to the Customer

Taking into account the nature of the Processing, Nous will provide reasonable assistance to the Customer, by appropriate technical and organizational measures, in responding to requests from Data Subjects seeking to exercise their rights, and in meeting the Customer's obligations relating to security, breach notification, data protection impact assessments, and consultation with supervisory authorities.

8. Personal Data Breach notification

Nous will notify the Customer without undue delay, and in any event within seventy two hours, after becoming aware of a Personal Data Breach affecting the Customer's Personal Data. The notification will describe, to the extent known, the nature of the breach, the likely consequences, and the measures taken or proposed to address it.

9. Return and deletion of data

Upon termination or expiry of the Agreement, and at the choice of the Customer, Nous will delete or return the Personal Data it Processes on the Customer's behalf, and delete existing copies, unless retention is required by law. Deletion of a workspace in the application removes the associated records from the primary systems in the ordinary course.

10. Audit and information

Nous will make available to the Customer information reasonably necessary to demonstrate compliance with this DPA, including third party assessments and certifications where available. Where the Customer reasonably requires further audit, the parties will agree on scope, timing, and cost in advance, subject to confidentiality and to not disrupting the Service or other customers.

11. International transfers

Where Nous transfers Personal Data originating in the European Economic Area, the United Kingdom, or Switzerland to a country not recognized as providing an adequate level of protection, the transfer will be governed by an appropriate transfer mechanism, such as the European Commission Standard Contractual Clauses, which are incorporated by reference where applicable.

12. Liability

Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the Agreement.

13. Term, conflict, and governing law

This DPA remains in effect for as long as Nous Processes Personal Data on behalf of the Customer. In the event of a conflict between this DPA and the Agreement regarding the Processing of Personal Data, this DPA prevails. This DPA is governed by the law and jurisdiction set out in the Agreement, unless Applicable Data Protection Law requires otherwise.

Signatures

Processor	**Controller (Customer)**
Name and title	Name and title
Signature	Signature
Date	Date

Annex I: Description of Processing

Item	Detail
Categories of Data Subjects	The Customer's contacts, prospects, leads, customers, and the Customer's own personnel whose data appears in the connected sources.
Categories of Personal Data	Names, business contact details, email content and metadata, calendar events, CRM records, meeting and call transcripts, messaging and engagement activity, and enrichment attributes, in each case limited to the integrations the Customer connects.
Special categories of data	Not intended. The Customer should not use the Service to Process special categories of data.
Nature and purpose	To unify signals from the Customer's connected sources into a context graph, and to serve resolved context to the Customer's authorized applications and agents.
Duration	For the term of the Agreement and until deletion in accordance with Section 9.
Frequency	Continuous, as data flows from the connected sources.

Annex II: Technical and Organizational Measures

Nous maintains measures that include, at minimum:

Area	Measure
Encryption in transit	All traffic is served over TLS, including HTTP/3, with certificates automatically provisioned and renewed.
Encryption at rest	The managed database encrypts data at rest. Sensitive credentials such as OAuth tokens are additionally encrypted at the application layer using AES 256 before storage.
Authentication	Access to connected sources uses OAuth. Nous does not request or store end user passwords for connected services.
Tenant isolation	Each customer's data is scoped to its own workspace, and access is controlled so that one customer cannot access another customer's data.
Integrity of inbound events	Inbound integration webhooks are validated with per integration signature secrets (HMAC).
Access control	Administrative access is restricted, granted on a need to know basis, and protected by multi factor authentication on administrative accounts.
Supply chain and code integrity	Automated secret scanning runs in continuous integration. The source code is open and version controlled, and repository history was audited before public release.
Monitoring	Automated integrity sweeps record the health of each workspace and flag new issues.
Deletion	Deletion of a workspace removes associated records from primary systems.

Annex III: Approved Subprocessors

Subprocessor	Purpose	Location
Supabase	Database and authentication hosting	United States
Anthropic	AI extraction via API (no training on Customer data)	United States
Stripe	Billing and payments	United States
Resend	Transactional and invitation email	United States
PostHog	Product analytics	United States
Connected integrations	Engaged only when the Customer connects them (for example Google Gmail and Calendar, Slack, Salesforce, HubSpot, Attio, Fireflies, Fathom, Calendly, Cal.com, LinkedIn connectivity, Apify, Apollo, and email verification, enrichment, and outbound providers)	Various

The current authoritative list is published at opennous.cloud/subprocessors.