# JANUS LABS INC.

## Sylph Privacy Policy

PP-001

| | |
|---|---|
| **Classification:** | Public |
| **Version:** | 1.5 |
| **Effective Date:** | October 14, 2026 |
| **Author:** | Akshat Sabavat |
| **Approved By:** | Akshat Sabavat, Benjamin Faibussowitsch |
| **Next Review:** | September 20, 2027 |

This document is the property of Janus Labs Inc. and is published for public reference.
It describes how Sylph collects, uses, and protects personal information.

Published at https://legal.januslabsinc.com/sylph/v1/

## Document Control

| Version | Date | Description | Author |
|---|---|---|---|
| 1.0 | May 28, 2026 | Initial release | Akshat Sabavat |
| 1.1 | May 28, 2026 | SMS consent and transactional messaging alignment; legal hosting URL | Akshat Sabavat |
| 1.2 | August 7, 2026 | Receipt submission by SMS covered; booking processor corrected to Duffel; editorial fixes | Akshat Sabavat |
| 1.3 | August 7, 2026 | Privacy contact points consolidated to akshat-sabavat@januslabsinc.com | Akshat Sabavat |
| 1.4 | September 20, 2026 | Sylph Solo covered; service providers and data categories brought up to date (AI providers, PKFares, PostHog, QuickBooks Online added; WhatsApp and single sign-on references removed); product analytics storage, AI processing, and de-identified data use described; retention aligned with the Terms of Service | Akshat Sabavat |
| 1.5 | October 14, 2026 | How to disconnect QuickBooks Online and what happens to accounting data afterwards | Akshat Sabavat |

## Contents

**Document Control** 1

**1 Introduction** 3

**2 Information We Collect** 3
- 2.1 Account Information . . . 3
- 2.2 Financial and Expense Data . . . 3
- 2.3 Travel Data . . . 4
- 2.4 Accounting Data . . . 4
- 2.5 Sylph Solo Data . . . 4
- 2.6 Usage and Technical Data . . . 4
- 2.7 Communication Data . . . 5
- 2.8 SMS Messaging and Consent Data . . . 5

**3 How We Use Your Information** 6
- 3.1 Aggregated and De-identified Data . . . 6

**4 AI Processing** 6

**5 Financial Data Access via Plaid** 7
- 5.1 What Data We Access . . . 7
- 5.2 Why We Access This Data . . . 7
- 5.3 Plaid's Own Privacy Practices . . . 7

5.4 Revoking Plaid Access . . . . . 7

**6 How We Share Your Information** **8**
6.1 Your Organization . . . . . 8

**7 Data Security** **8**

**8 Data Retention** **9**

**9 Your Rights** **9**
9.1 Right to Know . . . . . 9
9.2 Right to Access . . . . . 10
9.3 Right to Correction . . . . . 10
9.4 Right to Deletion . . . . . 10
9.5 Right to Opt Out of Data Sharing . . . . . 10
9.6 SMS Consent . . . . . 10
9.7 Exercising Your Rights . . . . . 10

**10 California Privacy Rights (CCPA)** **10**

**11 International Users** **11**

**12 Children's Privacy** **11**

**13 Changes to This Policy** **11**

**14 Contact Us** **12**

# 1. Introduction

Janus Labs Inc. ("Janus Labs," "we," "us," or "our") operates Sylph, an AI-native corporate travel and expense management platform. This Privacy Policy explains how we collect, use, share, and protect information when you use our services at `app.sylph-product.com` and `api.sylph-product.com` (collectively, the "Service"). Sylph is offered in two forms, and this policy covers both:

- **Sylph for organizations.** We contract with organizations (employers), and the users are their administrators and employees. For the personal information in an organization's account, the organization decides how it is used, and we process it on the organization's behalf as its service provider.
- **Sylph Solo.** Self-employed individuals and independent contractors sign up directly with us to organize their own business expenses. For Sylph Solo, we are the business responsible for your personal information.

Throughout this policy, "you" or "user" refers to any individual who interacts with the Service, whether as an organizational administrator, an employee, or a Sylph Solo user. Where a section applies to only one form of the Service, it says so.

By using Sylph, you agree to the collection and use of information as described in this policy. Your use of the Service is also governed by the Sylph Enterprise Terms of Service (`https://legal.januslabsinc.com/sylph/v1/terms`) or the Sylph Solo Terms of Service (`https://legal.januslabsinc.com/sylph/v1/solo-terms`), and, if your employer has enrolled in Sylph, by the agreement between your employer and Janus Labs. Related legal documents for Sylph are published at:

`https://legal.januslabsinc.com/sylph/v1/`

| | |
|---|---|
| **Legal entity** | Janus Labs Inc. |
| **Address** | 2653 North Hartland Court, Chicago, IL 60614 |
| **Contact** | Akshat Sabavat, CTO — akshat-sabavat@januslabsinc.com |

# 2. Information We Collect

We collect information in the following categories:

## 2.1 Account Information

When your organization creates your Sylph account, or when you sign up for Sylph Solo, we collect:

- Full name
- Email address
- Password (stored only in hashed form; we never store or have access to your plaintext password)
- Organization affiliation
- Role within your organization (administrator or employee)
- Mobile phone number associated with your account (when provided)

## 2.2 Financial and Expense Data

To provide expense management services, we collect:

- Bills and receipts (uploaded through the web application, or submitted via email or text message)
- Expense reports and associated metadata
- Company card metadata — specifically the last four digits of the card number, card network (e.g., Visa, Mastercard), and issuing bank name. **We never collect or store full card numbers (PANs).**
- Bank transaction history obtained through Plaid (see Section 5 for details)

### 2.3 Travel Data

When you use Sylph for travel booking and management, we collect:

- Trip requests and approval records
- Flight and hotel booking details (processed through our booking partners, Duffel and PKFares)
- Travel itineraries, including dates, destinations, and pricing
- Traveler details that airlines and hotels require to issue a booking: name as shown on identification, date of birth, gender, email address, and phone number
- For fares that require travel documents (generally international travel): nationality, and passport number, issuing country, and expiry date

### 2.4 Accounting Data

If your organization connects QuickBooks Online, we read its chart of accounts, classes, vendors, company information, and employee list (names and email addresses, used to set up employee accounts). We send to QuickBooks Online the journal entries, vendor records, and receipt images that your organization chooses to post, which may include employee and merchant names.

Your organization can disconnect QuickBooks Online at any time from Sylph's settings or from the Intuit app connections page. On disconnect we stop reading from and posting to the QuickBooks Online company file. Records already posted to QuickBooks Online remain there under your organization's control; the lists we read from it are deleted or de-identified within 90 days.

### 2.5 Sylph Solo Data

If you use Sylph Solo, we also collect:

- Your business profile: business name, business type (for example sole proprietor or single-member LLC), home state, a description of your work, business start date, whether your connected cards are used only for business or also personally, whether you use a home office or a vehicle for work, and your time zone
- Your accountant's name and email address, if you choose to provide them
- The names of your clients, if you choose to record them
- Mileage log entries you type in: date, start and end places, miles, and purpose. Sylph does not track your location.
- The tax category estimates the Service produces for your transactions, the corrections you make to them, and the date and version of the Terms you accepted

Sylph Solo does **not** ask for your Social Security number or taxpayer identification number.

### 2.6 Usage and Technical Data

We automatically collect certain technical information when you use the Service:

- Authentication events (login, logout, token refresh)
- IP addresses
- User agent strings (browser type and version)
- Product usage events, such as which features are used, recorded through our product analytics provider (PostHog) and linked to your user ID, organization, role, and email address

**Cookies and browser storage.** We do **not** use cookies or similar technologies for advertising, and we do not track you across other websites. We use two kinds of browser storage:

- Secure, HttpOnly authentication cookies that are required for the Service to function
- A first-party identifier that our product analytics provider stores in your browser (in a cookie and in local storage) so that we can measure how features of the Service are used. Session recording and automatic capture of clicks and keystrokes are turned off.

### 2.7 Communication Data

If you interact with Sylph or its AI assistant, we collect the content of communications submitted through supported channels, including:

- Web chat messages
- Email messages sent to Sylph service addresses, including the message body and any attachments such as receipts
- SMS messages sent to Sylph's messaging number, including receipt photos submitted by text and transactional account and security communications

These communications are processed solely to provide the requested Service, authenticate users, respond to requests, and improve the reliability and quality of the Service.

### 2.8 SMS Messaging and Consent Data

Sylph offers an optional, two-way transactional SMS messaging program for account security, receipt processing, and operational notifications. When you voluntarily consent to SMS messaging, we may collect and store:

- Mobile phone number associated with your account
- SMS consent status (for example, ACTIVE or REVOKED)
- Consent timestamp
- URL of the SMS Terms / disclosure in effect at the time of consent
- User agent and IP address associated with the consent action
- SMS delivery metadata (such as message timestamps and delivery status), where provided by our messaging provider

**Mobile phone numbers, SMS opt-in status, and SMS consent data are never sold, and are never shared with third parties or affiliates for marketing or promotional purposes.** This data is shared only with our SMS delivery provider, solely to deliver the messages described above.

Participation in SMS messaging is optional and requires explicit user consent collected through the Sylph application. Organizations cannot consent on behalf of individual users. Additional information is available in the **Sylph Transactional SMS Terms**, published at https://legal.januslabsinc.com/sylph/v1/.

# 3. How We Use Your Information

We use the information we collect for the following purposes:

- **Providing the Service** — processing expense reports, matching transactions to receipts, managing travel bookings, and enforcing organizational expense policies
- **Authentication and security** — verifying your identity, maintaining session security, protecting against unauthorized access, and sending multi-factor authentication (MFA) codes, login verification requests, and password reset codes
- **Communication** — sending transactional notifications related to your expenses, trips, bookings, account activity, security alerts, and other important operational communications
- **SMS transactional messaging** — where you have consented, sending SMS messages for authentication, receipt processing confirmations, expense-related notifications, security alerts, and important account or service notifications, and recording consent metadata for compliance and audit purposes
- **AI-assisted processing** — using optical character recognition and large language models to read receipts, extract expense data, evaluate policy compliance, suggest accounting codes, estimate tax categories in Sylph Solo, and respond to your messages and queries (see Section 4)
- **Service improvement** — identifying and fixing bugs, improving reliability, and enhancing features based on aggregated, non-identifying usage patterns
- **Legal compliance** — meeting our obligations under applicable laws and regulations

We do **not** use your information for advertising, marketing profiling, or selling to third parties. Sylph does not use the SMS program described in this policy to send advertisements, promotional campaigns, or unsolicited commercial communications.

## 3.1 Aggregated and De-identified Data

**We may create and use data that has been aggregated or de-identified so that it does not identify you, your organization, or any other individual, and cannot reasonably be linked back to them.** We use this data to measure, maintain, secure, and improve the Service, for example to understand usage volumes, error rates, and how accurately receipts are read. **This includes de-identified data derived from the bank and card transaction data we retrieve through Plaid.** We do not sell this data, and we do not attempt to re-identify it.

# 4. AI Processing

Much of what Sylph does relies on artificial intelligence. To provide these features, we send the relevant content to third-party AI providers, who process it on our behalf:

- **Mistral AI** reads the receipt images and documents you submit and converts them to text.
- **Anthropic** models extract expense details from that text, compare expenses to your organization's policy, suggest accounting codes, estimate tax categories in Sylph Solo, interpret text messages you send to Sylph, and power the AI assistant. Depending on the feature, the content sent can include receipt contents, merchant names, transaction amounts and dates, policy text, account names, and the messages you write.

**We do not use your information to train artificial intelligence models, and we do not permit our AI providers to do so.** They receive information only to produce results

for you or your organization.

Results produced by AI can be wrong. They are suggestions for people to review: your organization's administrators make the final decision on expenses, reports, and trips, and Sylph Solo users decide what to claim on their own tax returns. The Terms of Service say more about this.

## 5. Financial Data Access via Plaid

Sylph integrates with Plaid Inc. ("Plaid") to access your bank account transaction data. This section describes how that integration works and your rights regarding it.

### 5.1 What Data We Access

We use Plaid's **Transactions** product only. This provides us with your bank account transaction history, including transaction amounts, dates, merchant names, and categories. We do **not** use Plaid's Auth, Identity, Balance, or any other Plaid products. We do not access your bank account numbers, routing numbers, or account balances through Plaid.

### 5.2 Why We Access This Data

Transaction data obtained through Plaid is used only for the purposes below, and in aggregated or de-identified form as described at the end of this subsection:

- Matching bank transactions to submitted expense reports and receipts
- Supporting expense reconciliation workflows
- Helping your organization verify that reported expenses correspond to actual transactions
- In Sylph Solo, listing and sorting your transactions and estimating how each is likely to be treated for tax purposes

In Sylph Solo, if you connect a card or account that you also use for personal spending, we will receive those personal transactions as well. The Service tries to set them aside as personal.

We may also use transaction data in aggregated or de-identified form, as described in Section 3.1.

### 5.3 Plaid's Own Privacy Practices

When you connect your bank account through Plaid, Plaid collects and processes certain information according to its own privacy policy. We encourage you to review Plaid's end-user privacy policy at:

https://plaid.com/legal/#end-user-privacy-policy

### 5.4 Revoking Plaid Access

You may revoke Sylph's access to your bank transaction data at any time by:

1. Disconnecting the bank connection within Sylph's settings
2. Contacting your organization's Sylph administrator (organization accounts)
3. Contacting us directly at akshat-sabavat@januslabsinc.com
4. Revoking access through Plaid's portal at https://my.plaid.com

Upon revocation, we will stop retrieving new transaction data. Previously retrieved transaction data that has already been matched to expense reports may be retained as part of your organization's expense records, subject to your organization's data retention practices.

# 6. How We Share Your Information

**We never sell your personal information.** We do not share your information for marketing or advertising purposes with any third party, and share information only with the following categories of service providers, solely to operate the Service:

| Service Provider | Purpose |
|---|---|
| Supabase | Database hosting (PostgreSQL with encryption at rest) |
| Plaid | Bank account transaction data aggregation |
| Duffel and PKFares | Flight and hotel booking processing. They pass traveler details to the airline or hotel you book. |
| Anthropic | AI processing of receipts, expenses, policies, messages, and assistant conversations (see Section 4) |
| Mistral AI | Optical character recognition of receipt images and documents |
| Intuit (QuickBooks Online) | Accounting system connection, when your organization connects it |
| PostHog | Product analytics (feature usage linked to user ID, organization, role, and email address; hosted in the United States) |
| Twilio | SMS message delivery for the transactional messaging program |
| Cloudflare | Content delivery network, scheduled background processing, and file storage (receipts, policy documents) |
| Amazon Web Services (AWS) | Application hosting, email delivery and inbound email processing (SES, S3), and background processing of receipts and reports (Lambda, Fargate) |
| Pydantic Logfire | Application performance monitoring and diagnostics. Telemetry is filtered to keep names, email addresses, and phone numbers out. Technical traces of document processing may incidentally contain receipt content. |

We may also disclose information if required by law, regulation, legal process, or governmental request, or if necessary to protect the rights, property, or safety of Janus Labs, our users, or the public.

## 6.1 Your Organization

For organizations that enable Sylph's optional SMS messaging service, authorized administrators may be informed when employees enable or disable SMS messaging or update the mobile phone number associated with their account. Organizational administrators can view employee expenses, trip requests, bookings, and policy compliance results. This access is a core function of the Service and is governed by your organization's own internal policies.

# 7. Data Security

We implement the following technical and organizational controls to protect your information:

| Control | Description |
|---|---|
| Encryption in transit | All client-server communication uses TLS 1.2 or higher |
| Encryption at rest | Database storage is encrypted via AES-256 (managed by Supabase). File storage in Cloudflare R2 uses server-side encryption. |
| Authentication | JWT-based authentication with short-lived access tokens (4-hour expiry) and refresh tokens (72-hour expiry), stored in secure, HttpOnly cookies |
| Access control | Role-based access control (RBAC) with strict tenant isolation — all data queries are scoped by organization, preventing cross-organization data access |
| Infrastructure security | Multi-factor authentication (MFA) is required on all infrastructure accounts (AWS, Supabase, GitHub, Cloudflare) |
| Log hygiene | Application telemetry passes through an allow-list filter designed to keep personal identifiers such as names, email addresses, and phone numbers out of logs and traces |

For additional detail on our security practices, please refer to our Information Security Policy (ISP-001), available upon request.

## 8. Data Retention

We retain your personal information for as long as necessary to provide the Service to your organization and to comply with our legal obligations, resolve disputes, and enforce our agreements. Specific retention periods vary by data type:

- **Account data** is retained for as long as the account is open.
- **Expense and travel records** are retained as long as the account is active, as these constitute business records that you or your organization may need for tax, audit, or compliance purposes.
- **SMS consent records** (status, timestamp, policy URL, and related metadata) are retained as needed for compliance, audit, and to honor opt-out requests.
- **Authentication logs** are retained for a limited period for security monitoring and incident investigation.

When an account is closed, or upon a valid deletion request, we will delete or de-identify the personal information in that account within **90 days**, except for copies in routine backups (which are overwritten on their normal cycle), records of travel bookings that suppliers or payment processors require us to keep, and other information we are required by law to keep. Data can be exported while an account is open and for 30 days after it is closed. Deletion is carried out on request to support@sylph-product.com.

## 9. Your Rights

Depending on your jurisdiction, you may have the following rights regarding your personal information:

### 9.1 Right to Know

You have the right to know what personal information we collect, how we use it, and with whom we share it. This policy is intended to satisfy this right. You may also request a copy of the specific personal information we hold about you.

### 9.2 Right to Access

You may request access to the personal information we have collected about you. Much of this information is already accessible directly through the Sylph application (your profile, expenses, trips, and bookings).

### 9.3 Right to Correction

You have the right to request correction of inaccurate personal information. You can update most account information directly within Sylph, or contact your organization's administrator for assistance.

### 9.4 Right to Deletion

You may request that we delete your personal information, subject to certain exceptions (such as data we are required to retain for legal or compliance purposes, or data that constitutes part of your organization's business records).

### 9.5 Right to Opt Out of Data Sharing

You have the right to opt out of the sale or sharing of your personal information for targeted advertising. However, **we do not sell your personal information or share it for advertising purposes**, so this right is satisfied by default.

### 9.6 SMS Consent

Where you have consented to SMS messaging, you may withdraw that consent at any time by replying **STOP** to any Sylph SMS message, or by revoking consent in your Sylph account settings (where available). Withdrawing SMS consent does not affect your ability to use Sylph through non-SMS channels.

### 9.7 Exercising Your Rights

To exercise any of these rights, please contact:

- Your organization's Sylph administrator (for organization-managed data)
- Akshat Sabavat, CTO — akshat-sabavat@januslabsinc.com (for requests directly to Janus Labs)

We will respond to verified requests within 45 days. If we need additional time, we will notify you of the extension and the reason. If you use Sylph through your employer, certain requests (particularly deletion requests) may need to be coordinated with your organization, as your employer is the data controller for much of the information processed through Sylph. If you use Sylph Solo, contact us directly, as we are responsible for your information.

## 10. California Privacy Rights (CCPA)

If you are a California resident, the California Consumer Privacy Act (CCPA) provides you with additional rights:

- **Right to know** the categories and specific pieces of personal information we have collected
- **Right to delete** your personal information, subject to certain exceptions
- **Right to opt out** of the sale of personal information — we do not sell personal information

- **Right to non-discrimination** — we will not discriminate against you for exercising your CCPA rights

**Categories of personal information collected** (as defined by the CCPA):

- Identifiers (name, email address, phone number, IP address)
- Financial information (bank transaction history via Plaid, expense data, company card metadata)
- Commercial information (travel bookings, expense reports)
- Government identification details (passport number, issuing country, and expiry date, only where a travel booking requires them), which are sensitive personal information and are used only to make that booking
- Characteristics required by travel suppliers (date of birth, gender, nationality)
- Professional information (for Sylph Solo: business profile, client names, and mileage log)
- Internet or electronic network activity (authentication events, user agent strings, product usage events)
- SMS consent and related transactional messaging metadata, where applicable

In the preceding 12 months, we have **not** sold any personal information, and we have **not** shared personal information for cross-context behavioral advertising. To submit a CCPA request, contact us at akshat-sabavat@januslabsinc.com.

## 11. International Users

Janus Labs is based in the United States, and the Service is offered only to organizations and individuals in the United States. If you nevertheless access the Service from outside the United States, please be aware that your information will be transferred to, stored, and processed in the United States, where data protection laws may differ from those in your jurisdiction. If you are located in the European Economic Area (EEA), the United Kingdom, or another jurisdiction with data protection laws that provide rights similar to the General Data Protection Regulation (GDPR), you may have additional rights including the right to lodge a complaint with your local data protection authority. We process personal information on the basis of contractual necessity (to provide the Service to your organization), legitimate interests (to maintain security and improve the Service), and consent (where required by law, including SMS consent). For any questions about international data transfers, contact us at akshat-sabavat@januslabsinc.com.

## 12. Children's Privacy

Sylph is a business product designed for use by employees of organizations and by self-employed adults. You must be at least 18 years old to use the Service. We do not knowingly collect personal information from children under the age of 16. If we become aware that we have collected personal information from a child under 16, we will take steps to delete that information promptly.

## 13. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, or legal requirements. When we make material changes:

- We will update the "Effective Date" at the top of this policy
- We will notify organizational administrators and Sylph Solo users via email

- For significant changes affecting how we collect or share personal information, we will provide at least 30 days' notice before the changes take effect

Updated versions are published at https://legal.januslabsinc.com/sylph/v1/. We encourage you to review this policy periodically. Your continued use of the Service after any changes indicates your acceptance of the updated policy.

## 14. Contact Us

| | |
|---|---|
| **Privacy & Security** | Akshat Sabavat, CTO — akshat-sabavat@januslabsinc.com |
| **Mailing address** | Janus Labs Inc., 2653 North Hartland Court, Chicago, IL 60614 |

End of Document — Janus Labs Inc. — PP-001 v1.5