sherpa

← Back to Home

Privacy Policy

Effective Date: May 18, 2026 **Last Updated:** May 18, 2026 **Version:** 1.1

1. Definitions

For purposes of this Privacy Policy:

- **Personal Information** or **Personal Data** means any information relating to an identified or identifiable individual, including but not limited to name, email address, IP address, and usage data.
- **Services** means Sherpa's AI-powered Cloud Operational Platform and all related features, tools, and functionalities.
- **Customer Data** means AWS configuration data, cost and usage reports, resource metadata, and security findings analyzed by our platform.
- **Account Data** means information related to your Sherpa account, including authentication credentials and profile settings.
- **Processing** means any operation performed on Personal Data, including collection, storage, use, disclosure, or deletion.

2. Our Company and Mission

Sherpa is the centralized place to talk to your AWS cloud — applications and infrastructure together, across cost, security, observability, and other operations. Use Sherpa as a dashboard to see what's happening, or have a conversation about it. Beyond day-to-day visibility, Sherpa helps you make informed decisions about your cloud — whether you're optimizing what you have or evaluating bigger changes like modernization, migration, or contractor onboarding.

Our Mission: To make AWS operations clear, conversational, and actionable — so every team running on AWS, regardless of size, can see what they have, ask anything about it, and act with confidence.

3. Introduction

This Privacy Policy describes how we collect, use, and disclose information when you interact with our platform. We are committed to protecting your personal information and ensuring your experience is secure and professional. This policy applies to all users of Sherpa's Services. We comply with applicable US state privacy laws such as CCPA/CPRA, and we are working toward alignment with GDPR for EU data protection.

4. Information We Collect

We collect information that identifies you or relates to your AWS cloud operations on our platform. The data collected varies based on your user role:

For Platform Administrators:

- Contact information (name, business email, phone number)
- Company profiles and organizational details
- AWS account configurations and integration preferences
- Billing and payment information

For Team Members:

- Professional identifiers and role information
- Role-based access permissions and security settings
- Usage patterns and optimization preferences
- Activity logs and interaction history

Customer Data (AWS Environment Information):

- AWS Cost and Usage Reports (CUR)
- CloudTrail logs and API activity
- AWS Config data and resource configurations
- Security findings and compliance status
- Resource metadata and tagging information
- Performance metrics and utilization data

Technical Information:

- IP addresses and device identifiers
- Browser types and operating system information
- Log data and system diagnostics
- API calls and integration activity
- Performance metrics and error reports

Communication Data:

- Support tickets and help desk interactions
- Chat logs and email correspondence
- Feedback and survey responses
- Product usage inquiries

For All Users:

- **Account Data:** Authentication credentials, profile settings, and preferences
- **Activity Data:** Platform interaction telemetry, feature usage patterns, and session information

5. Cookies and Tracking Technologies

Our platform uses cookies and similar tracking technologies to keep you signed in, monitor platform performance, and understand usage. Categories used:

- **Authentication cookies (essential):** First-party cookies that store your sign-in session via AWS Cognito. Required for the platform to function. Disabling these will sign you out.
- **Performance cookies (analytics):** Where deployed, performance monitoring captures page-load times, errors, and HTTP behavior so we can keep Sherpa fast and reliable. First-party.
- **Third-party analytics cookies:** Where deployed, we may use third-party analytics services to understand aggregated usage patterns. These cookies may collect information about your device and usage behavior.
- **Functional cookies:** Where applicable, cookies that remember your preferences (theme, layout, dismissed notifications).

You can manage non-essential cookies through our in-product cookie consent banner or via your browser settings.

Global Privacy Control (GPC): We honor browser-level opt-out signals such as Global Privacy Control as valid opt-out-of-sale-or-sharing requests under applicable US state privacy laws.

6. How We Use Your Information

Your data is used specifically to fulfill our mission and operate the platform:

To Enable Cloud Optimization:

- Analyzing your AWS usage patterns to deliver actionable recommendations through our AI Agents and knowledge graph
- Generating cost optimization insights and security recommendations
- Creating customized roadmaps for cloud infrastructure improvements
- Identifying resource inefficiencies and optimization opportunities

Operational Communications:

- Sending critical platform updates and security alerts
- Providing account notifications and billing information
- Delivering optimization alerts and recommendation summaries
- Responding to support requests and inquiries

Security & Trust:

- Verifying identity to prevent fraud and unauthorized access
- Maintaining a safe environment for all users
- Detecting and preventing security threats
- Ensuring compliance with security standards

Platform Optimization:

- Analyzing aggregated, de-identified data to enhance our AI algorithms
- Improving recommendation accuracy and relevance

- Developing new features and product enhancements
- Conducting research and development activities

Legal Compliance:

- Fulfilling legal obligations and regulatory requirements
- Responding to legal requests and court orders
- Enforcing our Terms of Service and policies
- Protecting our rights and interests

7. Legal Basis for Processing (GDPR)

As we work toward full GDPR alignment, for users in the European Economic Area (EEA), United Kingdom, and Switzerland we process Personal Data based on the following legal grounds:

- **Contract performance** to provide our Services and fulfill contractual obligations
- **Legitimate interests** for platform improvement and security monitoring provided these interests are not overridden by your rights
- **Consent** for marketing communications and optional features which you may withdraw at any time
- **Legal obligations** to comply with applicable laws and regulations

8. Our Role and Yours (Controller and Processor)

For Customer Data (your AWS environment data analyzed by Sherpa), you are the Data Controller and Sherpa acts as the Data Processor — meaning we process Customer Data only on your instructions and according to your configured integrations. You retain ownership and control of your Customer Data at all times.

For Personal Data we collect directly from you (your account details, billing info, support interactions), Sherpa is the Data Controller.

Data Processing Agreement (DPA): Enterprise customers may request a DPA that formalizes the Controller/Processor relationship, sub-processor obligations, and security commitments. Contact info@sherpa-agent.com to request a DPA.

9. Data Sharing and Third-Party Services

We do not sell your data. Sharing is limited to the functional requirements of a cloud operations platform. When team access is configured, relevant cloud usage data and recommendations are shared among authorized team members to facilitate optimization delivery.

Sub-processors. We engage trusted third-party service providers (sub-processors) including:

- Cloud infrastructure providers for hosting and storage (including AWS)
- Payment processors for billing management
- Analytics services for usage insights, where deployed
- Communication platforms for transactional emails
- Security monitoring tools for threat detection
- Customer support platforms for help desk services

A current list of named sub-processors is available on request — contact info@sherpa-agent.com. All sub-processors are contractually bound to maintain data confidentiality and security standards consistent with this Privacy Policy. Where required by enterprise contracts, we will provide advance notice of new sub-processors.

We may disclose Personal Data when required by law, court order, or government regulation, or when necessary to protect our rights, safety, or property. In the event of a merger, acquisition, or sale of assets, your Personal Data may be transferred to the acquiring entity, subject to the same privacy protections.

10. AI Training and Customer Data

Sherpa uses de-identified, aggregated Customer Data to train and improve our AI models, so the platform delivers more accurate, context-aware recommendations over time. Your raw environment data is never shared or co-mingled with another customer's; only aggregated, de-identified signals contribute to model improvement.

What we train on:

- AWS configuration and resource metadata

- Cost and usage reports
- Security findings and compliance posture
- Observability signals
- Aggregated, de-identified usage telemetry

What we do NOT include in model training:

- Authentication credentials, passwords, or session tokens
- Direct identifiers from your account (your name, email address, billing info)
- AWS access keys or secrets

Where possible, we aggregate and de-identify Customer Data before it enters the training pipeline, so that individual account identifiers are not retained.

Your control:

- You retain ownership of your Customer Data at all times. Our use of de-identified, aggregated data for model improvement does not transfer ownership.
- Enterprise customers can discuss data-use terms, including model-training scope, as part of a Data Processing Agreement — contact info@sherpa-agent.com.

11. AWS Integration Disclosures

Sherpa's platform integrates with your AWS environment to provide visibility, recommendations, and (where you authorize them) automated actions. Sherpa connects to your AWS account through scoped IAM roles. Where Sherpa takes an action on your behalf — for example, single-click remediations or automated workflows — those actions use write permissions only with your explicit, scoped approval. You maintain full control over access permissions and can revoke access at any time.

We analyze:

- AWS Cost and Usage Reports for cost optimization
- CloudTrail logs for activity monitoring
- AWS Config data for resource configuration analysis
- Security Hub findings for security recommendations
- CloudWatch metrics for performance analysis

- Resource tags and metadata for organization insights

Security Measures:

- AWS credentials are encrypted using industry-standard encryption
- Access tokens are short-lived and automatically rotated
- All API calls use AWS Signature Version 4 authentication
- Credentials are never stored in plain text

Customer Data is processed in AWS regions based on your account configuration, and you can specify preferred regions for data residency. While Sherpa analyzes your AWS environment, you retain ownership and control of your AWS resources, and Sherpa's recommendations require your approval before implementation.

12. Automated Decision-Making and AI

Sherpa uses AI-powered algorithms to analyze your AWS environment and generate recommendations. Our AI Agents analyze AWS usage patterns, cost data, and security configurations, with recommendations generated using machine learning models trained on cloud optimization best practices.

The knowledge graph connects disparate AWS data points to identify optimization opportunities using hybrid search mechanisms combining vector and keyword matching to improve accuracy, with model evaluation including methodology specifics for precision and recall metrics.

All AI-generated recommendations are presented to you for review and approval, and no automated changes are made to your AWS environment without explicit authorization.

You have the right to:

- Understand how AI recommendations are generated
- Contest automated decisions
- Request human review of recommendations

13. International Data Transfers

Sherpa operates globally and may transfer Personal Data across international borders. Personal Data may be processed in the United States and other countries

where our service providers operate.

For transfers of Personal Data from the EEA, UK, or Switzerland to countries without adequate data protection laws, we use:

- Standard Contractual Clauses approved by the European Commission
- AWS Data Processing Addendum for cloud infrastructure
- Other legally approved transfer mechanisms

Enterprise customers may specify preferred AWS regions for data storage and processing to meet local data residency requirements.

14. Data Retention

We retain Personal Data only as long as necessary for the purposes described in this Privacy Policy.

- **Active account data** is retained for the duration of your service relationship with Sherpa
- **AWS analysis data** including cost and usage data is retained for 24 months to enable trend analysis and historical comparisons
- **Security findings** are retained for 12 months
- **Backup copies** are retained for 90 days for disaster recovery purposes

Upon account deletion, Personal Data is retained for 30 days to allow for account recovery, then permanently deleted within 90 days. Data may be retained longer when required by law, regulation, or legal proceedings. We may retain anonymized, aggregated data indefinitely for research and product improvement purposes.

15. Data Security

We implement industry-standard security measures to protect your Personal Data from unauthorized access, disclosure, alteration, and destruction. Our security practices include:

- Encryption of data in transit and at rest
- Access controls and authentication requirements
- Regular security monitoring and assessments

- Employee training on data protection

We maintain strict internal access controls to ensure your information is only accessible by personnel necessary for support or security operations. While we strive to protect your Personal Data, no method of transmission or storage is completely secure, and we cannot guarantee absolute security.

16. Data Breach Notification

In the event of a data breach affecting your Personal Data, we will notify affected users within 72 hours of discovering a breach, as required by GDPR and applicable laws.

Breach notifications will include:

- The nature of the breach and data affected
- Potential consequences and risks
- Measures taken to address the breach
- Recommended actions for affected users
- Contact information for questions

We will take immediate steps to contain the breach, investigate the cause, and implement measures to prevent future incidents. We will notify relevant supervisory authorities as required by applicable data protection laws.

17. Your Rights

You have the following rights regarding your Personal Data:

- **Right to access** and request a copy of your Personal Data within 30 days
- **Right to rectification** to update or correct inaccurate information
- **Right to erasure** to request deletion subject to legal retention requirements
- **Right to restrict processing** in certain circumstances
- **Right to data portability** to receive your data in a structured machine-readable format
- **Right to object** to certain processing activities including marketing communications

- **Right to withdraw consent** at any time without affecting prior lawful processing
- **Right to lodge a complaint** with your local data protection supervisory authority if you believe your rights have been violated

To exercise any of these rights, contact us at info@sherpa-agent.com, and we will respond within 30 days and may require identity verification.

18. US State Privacy Rights

If you are a resident of California, Virginia, Colorado, Connecticut, Texas, Utah, or another US state with a comprehensive consumer privacy law in effect, you have additional rights regarding your Personal Information. Sherpa applies these rights to all eligible residents under the relevant state law:

Categories of Personal Information we collect include identifiers, commercial information, internet and network activity, geolocation data, professional information, and inferences drawn from the above. We collect this information for the business purposes outlined in Section 6 (providing and improving Services, customer support, security and fraud prevention, legal compliance, research and development).

We do not sell Personal Information. We have not sold Personal Information in the preceding 12 months and do not share Personal Information for cross-context behavioral advertising.

Your rights as a US state resident (specific rights vary by state but generally include):

- The right to know what Personal Information is collected, used, and disclosed
- The right to access or obtain a portable copy of your Personal Information
- The right to correct inaccurate information
- The right to delete Personal Information, subject to legal retention requirements
- The right to opt out of sale, sharing, or targeted advertising (not applicable — we don't sell or share for advertising)
- The right to limit use of sensitive Personal Information
- The right to non-discrimination for exercising these rights
- The right to appeal a denied request (Virginia, Colorado, Connecticut, Texas, others)

Global Privacy Control (GPC). We honor browser-level opt-out signals such as Global Privacy Control as valid opt-out-of-sale-or-sharing requests under applicable state laws.

Authorized agents. You may designate an authorized agent to make requests on your behalf by providing written authorization. We will verify your identity before processing requests by matching information you provide with information in our records. Contact us at info@sherpa-agent.com to exercise your rights or to confirm we do not sell or share Personal Information.

19. Children's Privacy

Sherpa's Services are not directed to individuals under the age of 16. We do not knowingly collect Personal Information from children. If we discover that we have collected Personal Information from a child without parental consent, we will delete that information immediately. If you believe we have collected information from a child, please contact us at info@sherpa-agent.com.

20. Marketing Communications

We may send you marketing communications about Sherpa's Services, features, and updates including:

- Product announcements
- Educational content
- Webinars and events
- Promotional offers

You can manage your communication preferences through your account settings or by clicking "unsubscribe" in any marketing email, though you cannot opt-out of transactional or service-related communications. Marketing emails are sent no more than twice per week unless you opt-in to more frequent communications. We do not share your information with third parties for their marketing purposes.

21. Compliance and Security Standards

Sherpa is committed to maintaining industry-standard security practices and data protection compliance. Our platform aligns with:

- **US state consumer privacy laws** (CCPA/CPRA + Virginia, Colorado, Connecticut, Texas, Utah, and other applicable state laws)
- **AWS Partner Network** security standards for cloud infrastructure

We are **actively pursuing SOC 2 Type II certification** and **working toward GDPR alignment** for EU data protection. We implement security controls aligned with the SOC 2 framework while certification is in progress. As we grow, we will obtain additional compliance certifications to meet enterprise customer requirements. Information about our current security practices and compliance roadmap is available upon request — contact info@sherpa-agent.com.

22. Changes to Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our practices or legal requirements. We will notify you of material changes by:

- Email notification to your registered email address
- Prominent notice on our platform
- In-app notification upon login

Changes become effective 30 days after notification, unless otherwise required by law. Changes that significantly affect your rights or how we process Personal Data will require your consent before taking effect. Previous versions of this Privacy Policy are available upon request.

23. Contact Information

For privacy-related inquiries, data subject requests, security reports, or general questions, please contact us:

Email: info@sherpa-agent.com **Response time:** Within 30 days of request

Mailing Address: Sherpa, Inc. 156 9th St Woodridge, NJ 07075 United States

Supervisory Authority: If you are located in the EEA, you have the right to lodge a complaint with your local data protection authority. A list of authorities is available at: edpb.europa.eu/about-edpb/board/members_en

Acknowledgment

By using Sherpa's Services, you acknowledge that you have read, understood, and agree to this Privacy Policy.