

Privacy Policy

OpsFusion LLC State of California, United States

Effective Date: July 17, 2026 **URL:** <https://opsfusion.cloud/privacy>

This Privacy Policy describes how OpsFusion LLC (“OpsFusion,” “we,” “us,” or “our”) collects, uses, shares, and protects information in connection with our on-call and incident alerting platform (the “Service”). This Privacy Policy applies to all users of the Service, including account administrators, team members, and other Authorized Users.

By accessing or using the Service, you acknowledge that you have read and understood this Privacy Policy. If you are using the Service on behalf of an organization, you represent that you are authorized to accept this Privacy Policy on behalf of that organization.

1. Information We Collect

1.1 Account and Contact Information

When you register for or use the Service, we collect:

- **Identity information:** Full name, username, email address
- **Authentication information:** Account credentials (encrypted), OAuth provider details (e.g., Google, GitHub), single sign-on tokens
- **Contact information:** Phone number(s) for SMS and voice call notifications
- **Organizational information:** Company or organization name, account role, team memberships

1.2 Alert and Incident Data

In the course of providing the Service, we process:

- **Alert content:** Alert titles, descriptions, labels, severity levels, and associated metadata
- **Routing and escalation data:** Team assignments, on-call schedules, escalation policies, notification preferences
- **Notification logs:** Records of notification delivery attempts, delivery status, and channel used (email, SMS, voice)
- **Incident timeline data:** Acknowledgment, closure, and status change timestamps and actors

1.3 Technical and Usage Information

We automatically collect:

- **Device and browser information:** IP address, browser type and version, operating system, device type
- **Usage data:** Pages visited, features used, API calls made, clickstream data
- **Log data:** Server logs, error logs, access timestamps, referring URLs
- **Performance data:** Page load times, API response times, error rates

1.4 Billing Information

Payment and billing information is collected and processed by Paddle, our merchant of record. OpsFusion does not directly collect, store, or process credit card numbers, bank account details, or other payment instrument data. We receive from Paddle: subscription status, plan tier, billing cycle dates, transaction identifiers, and billing contact information.

1.5 Communications

We collect information from communications you send to us, including support requests, feedback, and correspondence via email or in-app messaging.

2. How We Use Information

We use the information we collect for the following purposes:

2.1 Service Delivery

- Provide, operate, and maintain the on-call scheduling and alerting Service
- Deliver notifications via email, SMS, and voice calls
- Process and route alerts according to your configurations
- Manage your account, subscriptions, and billing

2.2 Service Improvement

- Analyze usage patterns to improve Service performance and reliability
- Develop new features and functionality
- Generate aggregated, anonymized analytics and benchmarks
- Diagnose and fix technical issues

2.3 Communication

- Send transactional communications (account verification, password resets, billing receipts)
- Provide Service-related notifications (maintenance windows, incident reports, feature updates)
- Respond to support requests and inquiries

2.4 Security and Compliance

- Detect, prevent, and investigate security incidents, fraud, and abuse
- Enforce our Terms of Service and Acceptable Use Policy
- Comply with applicable legal obligations, including responding to lawful requests from public authorities

2.5 Legal Basis for Processing (GDPR)

For individuals in the European Economic Area (EEA), United Kingdom, or Switzerland, our legal bases for processing personal data are:

Purpose	Legal Basis
Service delivery	Performance of contract (Art. 6(1)(b) GDPR)
Billing and payments	Performance of contract (Art. 6(1)(b) GDPR)
Service improvement	Legitimate interests (Art. 6(1)(f) GDPR)
Security and abuse prevention	Legitimate interests (Art. 6(1)(f) GDPR)
Legal compliance	Legal obligation (Art. 6(1)(c) GDPR)
Marketing communications	Consent (Art. 6(1)(a) GDPR)

3. How We Share Information

We do not sell personal information. We share information only in the following circumstances:

3.1 Service Providers and Subprocessors

We share information with third-party service providers that assist in delivering the Service:

Provider	Purpose	Data Shared
Amazon Web Services (AWS)	Cloud hosting, compute, storage, email delivery (SES)	All Service data (encrypted at rest and in transit)
Twilio	SMS and voice call notification delivery	Phone numbers, notification content
Paddle	Payment processing, billing, merchant of record	Billing contact info, subscription details

3.2 Within Customer's Organization

Alert data, user information, and activity logs are visible to other Authorized Users within the same Customer account, subject to role-based access controls configured by the Customer.

3.3 Legal Requirements

We may disclose information when required by law, subpoena, court order, or governmental request, or when we believe in good faith that disclosure is necessary to: (a) comply with applicable law; (b) protect our rights, property, or safety; (c) prevent fraud or security threats; or (d) enforce our Terms of Service.

3.4 Business Transfers

In connection with a merger, acquisition, reorganization, bankruptcy, or sale of assets, your information may be transferred to the acquiring entity. We will provide notice of any such transfer and any choices you may have regarding your information.

3.5 With Consent

We may share information with third parties when you have provided explicit consent to do so.

4. Data Retention

We retain personal information only for as long as necessary to fulfill the purposes for which it was collected:

Data Type	Retention Period
Alert data	90 days from creation (configurable by plan)
Notification delivery logs	90 days
Audit logs	90 days
Account and user profile data	Duration of active subscription + 30 days
Billing and transaction records	7 years (legal/tax requirements)
Server and access logs	90 days

After the applicable retention period, data is permanently deleted or anonymized. Some data may be retained longer if required by applicable law or regulation.

5. Data Security

We implement industry-standard technical and organizational measures to protect your information:

5.1 Technical Measures

- **Encryption in transit:** All data transmitted between your browser and our servers is encrypted using TLS 1.2 or higher
- **Encryption at rest:** All data stored in our databases and storage systems is encrypted using AES-256 encryption
- **Access controls:** Role-based access controls with principle of least privilege for all systems
- **Infrastructure security:** Hosted on AWS with SOC 2 Type II certified infrastructure
- **API security:** All API endpoints authenticated; API keys hashed before storage
- **Authentication:** OAuth 2.0 / OpenID Connect via AWS Cognito with support for social identity providers

5.2 Organizational Measures

- Employee access to Customer Data is limited to authorized personnel with a business need
- Regular security reviews and infrastructure hardening
- Incident response procedures for security events
- Data processing agreements with all subprocessors

5.3 Security Incident Notification

In the event of a security breach affecting your personal information, we will notify you and any applicable regulatory authorities in accordance with applicable law. See Section 9 (Data Breach Notification) for details.

6. International Data Transfers

6.1 Processing Location

The Service is hosted on AWS infrastructure in the United States. By using the Service, your information may be transferred to, stored, and processed in the United States.

6.2 EU/UK Transfer Mechanisms

For transfers of personal data from the European Economic Area, United Kingdom, or Switzerland to the United States, we rely on:

- **Standard Contractual Clauses (SCCs):** We execute EU-approved SCCs with customers and subprocessors as required
- **Data Processing Agreement:** Our DPA incorporates the necessary transfer mechanisms. See <https://opsfusion.cloud/dpa>

6.3 Transfer Impact Assessment

We conduct transfer impact assessments to evaluate the level of data protection in recipient countries and implement supplementary measures where necessary.

7. Your Rights

7.1 EU/EEA/UK Residents' Rights (GDPR)

If you are located in the European Economic Area, United Kingdom, or Switzerland, you have the following rights under the General Data Protection Regulation (GDPR):

- **Restrict processing:** Request that we limit the processing of your personal data in certain circumstances
- **Object to processing:** Object to processing based on legitimate interests
- **Data portability:** Receive your personal data in a structured, commonly used, machine-readable format
- **Withdraw consent:** Where processing is based on consent, withdraw that consent at any time without affecting the lawfulness of prior processing
- **Lodge a complaint:** File a complaint with your local supervisory authority

7.2 California Residents' Rights (CCPA/CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

- **Right to know:** Request information about the categories and specific pieces of personal information we have collected, the sources of collection, the business purposes for collection, and the categories of third parties with whom we share information
- **Right to delete:** Request deletion of your personal information, subject to exceptions
- **Right to correct:** Request correction of inaccurate personal information
- **Right to opt-out of sale/sharing:** We do not sell or share personal information for cross-context behavioral advertising. No opt-out is necessary
- **Right to non-discrimination:** We will not discriminate against you for exercising your privacy rights
- **Right to limit use of sensitive personal information:** We do not use sensitive personal information for purposes beyond what is necessary to

provide the Service

Categories of Information Collected (for CCPA disclosure):

Category	Examples	Collected
Identifiers	Name, email, phone number, IP address	Yes
Commercial information	Subscription records, billing history	Yes
Internet/electronic activity	Usage data, log data, clickstream	Yes
Geolocation data	IP-based approximate location	Yes
Professional/employment information	Job title (if provided)	Optional
Sensitive personal information	Account credentials	Yes (for auth only)

We do not sell personal information. We do not share personal information for cross-context behavioral advertising.

7.3 Exercising Your Rights

To exercise any of the above rights, contact us at:

- **Email:** support@opsfusion.cloud
- **Subject line:** Include “Privacy Request” and the specific right you are exercising

We will respond to your request within thirty (30) days (or within the time-frame required by applicable law). We may need to verify your identity before processing your request. If you are an Authorized User acting on behalf of a Customer organization, we may direct your request to the Customer’s account administrator.

8. Cookies and Tracking Technologies

8.1 Cookies We Use

We use cookies and similar technologies to operate and improve the Service:

Cookie Type	Purpose	Duration
Strictly necessary	Authentication, session management, security	Session
Functional	User preferences, language settings	Persistent
Analytics	Usage patterns, Service performance	Persistent

8.2 Your Cookie Choices

You can control cookies through your browser settings. Disabling strictly necessary cookies may prevent you from using certain features of the Service. We do not use cookies for third-party advertising or cross-site tracking.

8.3 Do Not Track

The Service does not respond to “Do Not Track” browser signals, as there is no industry-standard protocol for such signals. However, we do not engage in cross-site tracking.

9. Data Breach Notification

9.1 Notification to Customers

In the event of a confirmed security breach involving unauthorized access to Customer Data, OpsFusion will notify affected customers without undue delay and in any event within seventy-two (72) hours of becoming aware of the breach, to the extent feasible.

9.2 Notification Content

Breach notifications will include, to the extent known: (a) the nature of the breach; (b) the categories and approximate number of individuals affected; (c) the likely consequences of the breach; (d) measures taken or proposed to address the breach; and (e) a point of contact for further information.

9.3 Regulatory Notification

OpsFusion will cooperate with Customer in notifying applicable regulatory authorities as required by law, including notifying the relevant supervisory authority within the timeframes required by GDPR and applicable U.S. state data breach notification laws.

10. Children’s Privacy

The Service is designed for business use and is not directed at individuals under the age of sixteen (16). We do not knowingly collect personal information from children under sixteen. If you believe we have inadvertently collected information from a child, please contact us at support@opsfusion.cloud and we will promptly delete such information.

11. Automated Decision-Making

OpsFusion does not use automated decision-making or profiling that produces legal effects or similarly significant effects on individuals. Alert routing and escalation decisions are based on configurations set by Customer administrators, not on automated profiling of individual users.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Material changes will be communicated via email or through the Service at least thirty (30) days before they take effect. The “Effective Date” at the top of this page indicates when the latest version became effective. Continued use of the Service after the effective date constitutes acceptance of the updated Privacy Policy.

13. Contact Information

For questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

OpsFusion LLC Email: support@opsfusion.cloud Website: <https://opsfusion.cloud>

For EU/EEA-related data protection inquiries, you may also contact our data protection representative at: support@opsfusion.cloud

This Privacy Policy was last updated on July 17, 2026.