Data Processing Agreement

OpsFusion LLC State of California, United States

Effective Date: July 17, 2026 **URL:** https://opsfusion.cloud/dpa

---

This Data Processing Agreement ("DPA") forms part of the Agreement between OpsFusion LLC ("OpsFusion," "Processor," "we," "us," or "our") and the Customer ("Controller," "you," or "your") that has entered into the Terms of Service available at https://opsfusion.cloud/terms (the "Principal Agreement").

This DPA applies to the extent that OpsFusion processes Personal Data on behalf of the Controller in the course of providing the Service. Terms not defined herein have the meaning set forth in the Principal Agreement.

---

1. Definitions

"Applicable Data Protection Law" means all data protection and privacy laws applicable to the processing of Personal Data under this DPA, including, without limitation, the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the UK General Data Protection Regulation ("UK GDPR"), the Swiss Federal Act on Data Protection ("FADP"), the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Act ("CPRA"), and any implementing or supplementary legislation.

"Controller" means the entity that determines the purposes and means of processing Personal Data (the Customer).

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable natural person that is processed by OpsFusion on behalf of the Controller in connection with the Service.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by OpsFusion.

"Processing" (and its cognates "Process" and "Processed") means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Processor" means the entity that processes Personal Data on behalf of the Controller (OpsFusion).

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission Decision 2021/914.

"Sub-processor" means any third party engaged by OpsFusion to process Personal Data on behalf of the Controller.

---

2. Scope and Roles

2.1 Roles

For the purposes of Applicable Data Protection Law:

- **Controller:** Customer determines the purposes and means of processing Personal Data through its configuration and use of the Service.
- **Processor:** OpsFusion processes Personal Data solely on behalf of and in accordance with the documented instructions of the Controller to provide the Service.

2.2 Scope of Processing

OpsFusion processes Personal Data solely to provide the Service as described in the Principal Agreement. The details of the processing are set forth in **Annex I** (Details of Processing).

---

3. Controller Obligations

3.1 Lawful Basis

Controller represents and warrants that: (a) it has obtained all necessary consents and/or has established a lawful basis for the processing of Personal Data by OpsFusion under this DPA; (b) it has provided all required notices to Data Subjects; and (c) its processing instructions to OpsFusion comply with Applicable Data Protection Law.

3.2 Instructions

Controller is responsible for ensuring that its instructions to OpsFusion regarding the processing of Personal Data are lawful and do not cause OpsFusion to violate any Applicable Data Protection Law. Controller acknowledges that OpsFusion's obligation is to process Personal Data in accordance with Controller's documented instructions, and that OpsFusion is not responsible for determining whether Controller's instructions comply with applicable law.

3.3 Telecommunications Compliance

Controller is solely responsible for ensuring that: (a) all alert recipients have provided appropriate consent to receive communications via SMS, voice call, or email; (b) alert content complies with applicable telecommunications laws, including the Telephone Consumer Protection Act (TCPA), CAN-SPAM Act, and similar legislation; and (c) opt-out and do-not-call requests are honored.

---

4. Processor Obligations

4.1 Processing Instructions

OpsFusion shall process Personal Data only on documented instructions from the Controller, including transfers to third countries, unless required by applicable law. If OpsFusion believes an instruction infringes Applicable Data Protection Law, OpsFusion will promptly notify the Controller.

4.2 Confidentiality

OpsFusion ensures that all personnel authorized to process Personal Data: (a) are subject to contractual or statutory confidentiality obligations; and (b) process Personal Data only as necessary to provide the Service.

4.3 Security

OpsFusion shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures are described in **Annex II** (Technical and Organizational Measures) and shall provide a level of security appropriate to the risk of processing.

4.4 Sub-processing

OpsFusion shall not engage any Sub-processor to process Personal Data without complying with the requirements of Section 6 (Sub-processors).

4.5 Data Subject Rights

OpsFusion shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law. OpsFusion will promptly forward any Data Subject request received directly to the Controller.

4.6 Assistance with Compliance

OpsFusion shall assist the Controller in ensuring compliance with its obligations under Articles 32 through 36 of the GDPR (or equivalent provisions under other Applicable Data Protection Law), taking into account the nature of processing and the information available to OpsFusion. This includes assistance with:

- Security of processing
- Data breach notification
- Data protection impact assessments
- Prior consultation with supervisory authorities

---

5. Personal Data Breach

5.1 Notification

OpsFusion shall notify the Controller without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller.

5.2 Notification Content

The notification shall include, to the extent available:

- A description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records concerned
- The name and contact details of OpsFusion's point of contact
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects

5.3 Cooperation

OpsFusion shall cooperate with the Controller and take commercially reasonable steps to assist in the investigation, mitigation, and remediation of the breach. OpsFusion shall assist the Controller in meeting its obligations to notify supervisory authorities and Data Subjects under Applicable Data Protection Law.

5.4 Documentation

OpsFusion shall document all Personal Data Breaches, including the facts relating to the breach, its effects, and the remedial actions taken.

---

6. Sub-processors

6.1 Authorized Sub-processors

Controller provides general authorization for OpsFusion to engage Sub-processors to process Personal Data on behalf of the Controller. The current list of Sub-processors is set forth in **Annex III** (Sub-processors) and is also available at https://opsfusion.cloud/subprocessors.

6.2 Sub-processor Obligations

OpsFusion shall ensure that each Sub-processor is bound by data protection obligations no less protective than those set forth in this DPA. OpsFusion remains fully liable to the Controller for the performance of each Sub-processor's obligations.

6.3 Changes to Sub-processors

OpsFusion shall notify the Controller at least thirty (30) days prior to adding or replacing a Sub-processor by updating the Sub-processor list and sending notice to the Controller's registered email address.

6.4 Objection Rights

If the Controller has a reasonable, documented objection to a new or replacement Sub-processor based on data protection grounds, the Controller shall notify OpsFusion in writing within fifteen (15) days of receiving notice. The parties shall work in good faith to resolve the objection. If the parties are unable to resolve the objection within thirty (30) days, the Controller may terminate the affected portion of the Service without penalty by providing written notice.

---

7. International Data Transfers

7.1 Transfer Mechanisms

Where Personal Data originating from the European Economic Area, United Kingdom, or Switzerland is transferred to a country that does not provide an adequate level of data protection, OpsFusion shall ensure that appropriate safeguards are in place, including:

- **Standard Contractual Clauses (SCCs):** The EU-approved SCCs (Commission Implementing Decision 2021/914) are hereby incorporated by reference into this DPA. For transfers from the EEA, Module Two (Controller to Processor) applies. For transfers from the UK, the UK International Data Transfer Addendum applies.
- **Supplementary Measures:** OpsFusion implements supplementary technical and organizational measures as described in Annex II to ensure the

transferred Personal Data is afforded an essentially equivalent level of protection.

7.2 Transfer Impact Assessment

OpsFusion has conducted a transfer impact assessment and determined that, considering the supplementary measures in place, the transferred Personal Data is adequately protected.

---

8. Audits

8.1 Audit Rights

OpsFusion shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits and inspections conducted by the Controller or an independent third-party auditor mandated by the Controller.

8.2 Audit Conditions

Audits shall be conducted: (a) no more than once per twelve (12) month period, unless required by a supervisory authority or triggered by a Personal Data Breach; (b) with at least thirty (30) days' prior written notice; (c) during normal business hours; (d) in a manner that minimizes disruption to OpsFusion's operations; and (e) subject to reasonable confidentiality obligations. The Controller shall bear the costs of any audit, except where the audit reveals material non-compliance by OpsFusion with this DPA.

8.3 Third-Party Certifications

OpsFusion may satisfy audit obligations by providing: (a) certifications or audit reports from independent third-party auditors (such as SOC 2 reports); (b) responses to reasonable written information requests; or (c) other documentation demonstrating compliance. The Controller shall consider such documentation in good faith as a reasonable alternative to an on-site audit.

---

9. Data Retention and Deletion

9.1 Retention

OpsFusion shall retain Personal Data only for as long as necessary to provide the Service and in accordance with the data retention periods set forth in the Privacy Policy.

9.2 Return and Deletion

Upon termination of the Principal Agreement, OpsFusion shall permanently delete all Personal Data processed on behalf of the Controller in accordance with the data retention policy set forth in the Privacy Policy, unless retention is required by applicable law.

9.3 Certification

Personal Data is automatically deleted through time-based expiration policies applied at the database level. Upon the Controller's written request, OpsFusion shall provide written confirmation that automated deletion policies are in effect and that the applicable retention period has elapsed.

---

10. Liability

10.1 Liability Cap

Each party's total aggregate liability under this DPA is subject to the limitations of liability set forth in the Principal Agreement.

10.2 Allocation

To the extent permitted by Applicable Data Protection Law, each party shall be liable for its own acts and omissions in connection with its obligations under this DPA.

---

11. Term and Termination

11.1 Term

This DPA takes effect on the Effective Date and remains in effect for the duration of the Principal Agreement. The DPA shall automatically terminate upon termination or expiration of the Principal Agreement, subject to Section 9 (Data Retention and Deletion).

11.2 Survival

Sections 5 (Personal Data Breach), 8 (Audits), 9 (Data Retention and Deletion), and 10 (Liability) survive termination of this DPA.

---

12. Miscellaneous

12.1 Precedence

In the event of a conflict between this DPA and the Principal Agreement, this DPA shall prevail with respect to the processing of Personal Data.

12.2 Governing Law

This DPA is governed by the same governing law as the Principal Agreement, except that the SCCs shall be governed as specified therein.

12.3 Severability

If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

Annex I: Details of Processing

Categories of Data Subjects

- Customer employees and contractors (account administrators, team members, on-call responders)
- Individuals whose contact information is included in alert notifications (notification recipients)

Categories of Personal Data

- Names, email addresses, phone numbers
- Usernames, account roles, team memberships
- Alert content (titles, descriptions, labels, metadata)
- Notification delivery logs (channel, status, timestamps)
- IP addresses, browser information, user agent strings
- Authentication tokens and OAuth provider identifiers

Sensitive Data

No special categories of personal data (as defined in Article 9 of the GDPR) are intentionally processed. If Controller includes sensitive data in alert content, Controller is solely responsible for ensuring a lawful basis exists for such processing.

Processing Operations

- Storage and retrieval of account and user data
- Processing and routing of alerts based on configured rules

- Delivery of notifications via email (AWS SES), SMS (Twilio), and voice calls (Twilio)
- Logging of notification delivery status
- Generation of audit trails and activity logs
- Aggregation and anonymization for analytics

Duration of Processing

Processing continues for the duration of the Principal Agreement, subject to the data retention periods specified in the Privacy Policy.

Annex II: Technical and Organizational Measures

1. Encryption

- **In transit:** TLS 1.2 or higher for all data transmissions
- **At rest:** AES-256 encryption for all data stored in databases and object storage

2. Access Controls

- Role-based access control (RBAC) for all systems
- Principle of least privilege enforced for internal access
- Multi-factor authentication required for administrative access
- API keys hashed before storage; transmitted only at creation time

3. Authentication and Identity Management

- OAuth 2.0 / OpenID Connect via AWS Cognito
- Support for federated identity providers (Google, GitHub)
- Session token management with automatic expiration

4. Infrastructure Security

- Hosted on AWS with SOC 2 Type II certified infrastructure
- Network segmentation and security groups
- Serverless architecture (AWS Lambda) eliminating server-level attack surface
- DynamoDB with point-in-time recovery enabled
- S3 versioning and encryption for all object storage

5. Monitoring and Logging

- CloudWatch monitoring for all services
- Structured logging with audit trails
- Automated alerting for anomalous activity

- Log retention in accordance with data retention policy

6. Data Minimization

- Collection limited to data necessary for Service delivery
- Automatic data deletion per retention schedule (90-day default for alerts)
- TTL-based expiration on temporary data (invitations, sessions)

7. Incident Response

- Documented incident response procedures
- Breach notification within 72 hours of awareness
- Post-incident review and remediation

8. Business Continuity

- Multi-availability-zone deployment on AWS
- Automated backups with point-in-time recovery
- Serverless architecture with automatic scaling

Annex III: Sub-processors

The following Sub-processors are authorized to process Personal Data on behalf of the Controller:

Sub-processor	Purpose	Location	Data Processed
Amazon Web Services, Inc.	Cloud infrastructure, compute, storage, email delivery (SES), authentication (Cognito), database (DynamoDB)	United States	All Service data
Twilio, Inc.	SMS and voice call notification delivery	United States	Phone numbers, notification content

Sub-processor	Purpose	Location	Data Processed
Paddle.com Market Ltd	Payment processing, subscription billing, merchant of record	United Kingdom / United States	Billing contact info, subscription details

---

This Data Processing Agreement was last updated on July 17, 2026.