Data Processing Agreement

Last updated: 03 March 2026

Between: Customer (Data Controller) and Opisense AS (Data Processor)
Organisation number: 936 578 195 | contact@opisense.com

This Data Processing Agreement ("DPA") is entered into pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) and governs the processing of personal data by Opisense AS on behalf of the Customer in connection with the provision of the Opisense platform.

1. PURPOSE, SCOPE AND LEGAL BASIS

1.1 Purpose

This DPA governs Opisense AS's ("Data Processor") processing of personal data on behalf of the Customer ("Data Controller") in connection with the provision of the Opisense platform ("the Service").

1.2 Entry into force

This DPA enters into force when the Customer registers for the Service and applies for as long as Opisense processes personal data on behalf of the Customer.

1.3 Legal basis

This DPA is prepared in accordance with:

- Regulation (EU) 2016/679 (GDPR)
- Norwegian Personal Data Act of 15 June 2018
- Norwegian Data Protection Authority (Datatilsynet) guidelines

1.4 Order of precedence

In the event of conflict between documents, the following order of precedence applies:

- Service Order Form
- This Data Processing Agreement (DPA)
- Master Services Agreement
- Terms of Service
- Privacy Policy and other Policies

2. DEFINITIONS

Term	Definition
Personal data	Information that can directly or indirectly identify a natural person.
Processing	Any operation performed on personal data, including collection, storage, use, disclosure or deletion.
Data Controller	The Customer, who determines the purposes and means of the processing.
Data Processor	Opisense AS, which processes personal data on behalf of the Customer.
Sub-processor	A third-party provider engaged by Opisense to perform processing activities.
Data subjects	Natural persons whose personal data is processed, including the Customer's employees, contractors and end-users.
Supervisory authority	Datatilsynet, the Norwegian Data Protection Authority.
EEA	The European Economic Area.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. NATURE, PURPOSE AND DURATION OF PROCESSING

3.1 Nature of processing

Opisense processes personal data by:

- Receiving data from the Customer's users, including voice input, text, documents, and other content submitted through the platform
- Processing data using AI systems for transcription, content generation, analysis, automation, and other platform functions
- Storing input data and generated output
- Automatic routing, classification, and analysis of content
- Generating metadata (timestamps, user ID, processing logs, etc.)

3.2 Purpose of processing

Personal data is processed solely for:

- Delivering the Service, including AI-powered workspace, automation, and integration functions, in accordance with the Customer's documented instructions
- Technical operation and maintenance of the Platform
- Security monitoring and troubleshooting
- Compliance with legal obligations

3.3 Duration

Processing runs from the registration date until the later of: (i) 60 days after termination of the customer relationship, or (ii) such longer period as is required by applicable law. All personal data is deleted or returned in accordance with Section 10 of this DPA.

3.4 Categories of data subjects

- The Customer's employees
- The Customer's contractors
- The Customer's customers (if the Customer chooses to process their data)
- The Customer's administrative users

4. TYPES OF PERSONAL DATA

4.1 Categories of personal data

Category	Data types
Identification data	Name, email address, phone number, user ID, IP address
Voice data	Audio recordings, voice input, transcriptions, language identification
Technical data	Log data (timestamps, actions), device information, browser information, API requests
Content data	Text and content generated from user input, AI-generated output, metadata about reports, workflows, and automations, routing information
Integration data	Data received from or sent to third-party systems connected through the platform, including content, metadata, and user identifiers

4.2 Special categories of personal data

Opisense does not intentionally collect or process special categories of personal data as defined under Article 9 of the GDPR. However, the Customer acknowledges that special category data (including but not limited to health information, biometric data, or data revealing racial or ethnic origin) may be incidentally captured through voice input, AI-generated content, or documents submitted to the platform.

Where such incidental capture occurs, the Customer is responsible for ensuring that a valid legal basis exists under Article 9 of the GDPR and that appropriate consent mechanisms or safeguards are in place. The Customer shall notify Opisense in writing if it becomes aware that special category data is being regularly processed through the platform. In all cases, Opisense shall apply appropriate technical and organisational safeguards in accordance with the GDPR and this DPA, including limiting access to such data and ensuring its prompt deletion in accordance with the retention schedules set out in Section 10.

5. DATA PROCESSOR OBLIGATIONS

5.1 Processing according to instructions

Opisense shall process personal data only in accordance with documented instructions from the Customer.

- Opisense shall not process personal data for any purpose other than those set out in this DPA and the Service Agreement, unless instructed otherwise by the Customer in writing.
- If Opisense receives an instruction that Opisense believes violates applicable law, Opisense shall immediately inform the Customer.
- Opisense shall not disclose personal data to third parties unless authorised by the Customer or required by law.

5.2 Documented instructions

Processing instructions shall be documented and shall include the scope, nature, purpose and duration of processing as set out in this DPA, the Terms of Service, the platform functions, and any written instructions from the Customer.

5.3 Confidentiality

Opisense shall:

- Ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality;
- Ensure appropriate training of staff members with access to personal data;
- Restrict access to personal data to those who need access to perform their duties.

5.4 Notification of material changes

Opisense shall notify the Customer in writing of any material changes to its processing activities, security measures, or sub-processors at least 30 days in advance. The Customer may object to such changes in accordance with Section 7.5.

6. SECURITY MEASURES

6.1 Technical security measures

Area	Measures
Encryption	TLS 1.3 for data in transit; AES-256 for data at rest; encrypted database connections
Access control	Multi-factor authentication (MFA) required for all administrative users and available for all platform users; role-based access control (RBAC) enforced across all platform functions; regular access reviews conducted quarterly
Network security	Firewall and intrusion detection; DDoS protection; network segmentation
Logging and monitoring	Security logging of all access; automated alerting on anomalies; log retention minimum 90 days
Data storage	Voice data stored in AWS Frankfurt (EU); automatic deletion of voice data after 7 days unless Customer opts for longer retention; daily backup with 30-day retention

6.2 Organisational security measures

Opisense shall:

- Implement and maintain appropriate data protection policies;
- Provide data protection training to all staff upon hiring and annually thereafter;
- Designate a Data Protection Officer where required by law, or, where a DPO is not legally required, designate a data protection contact with responsibility for coordinating data protection matters. The current data protection contact can be reached at privacy@opisense.com;
- Conduct regular reviews of its data protection measures at least annually;
- Implement and maintain documented incident response procedures.

6.3 Testing and Evaluation

Opisense shall conduct annual penetration testing and quarterly vulnerability assessments to evaluate and enhance the effectiveness of technical and organisational security measures.

7. SUB-PROCESSORS

7.1 General authorisation

The Customer authorises Opisense to engage sub-processors to deliver the Service, subject to the conditions set out in this Section.

7.2 Current sub-processors

Provider	Service	Location	Purpose
Amazon Web Services (AWS)	Cloud infrastructure	Frankfurt, Germany (EU)	Data storage and hosting
Clerk	Authentication	USA/EU (SCCs in place)	User authentication and identity management
Stripe	Payment processing	EU/USA (SCCs in place)	Invoicing and payments
Elevenlabs	Voice technology	USA (SCCs in place)	Voice transcription and synthesis
OpenAI	AI model provider	USA (SCCs in place)	AI inference for content generation and analysis
Anthropic	AI model provider	USA (SCCs in place)	AI inference for content generation and analysis
Vercel	Application hosting	USA (SCCs in place)	Application hosting and edge delivery
Convex	Backend infrastructure	USA (SCCs in place)	Backend database and real-time data
Ragie	RAG infrastructure	USA (SCCs in place)	Document indexing and retrieval
Recall	Meeting technology	USA (SCCs in place)	Meeting recording and transcription capture
Composio	Integration platform	USA (SCCs in place)	Integration orchestration
Resend	Email delivery	USA (SCCs in place)	Transactional email delivery
Axiom	Observability	USA (SCCs in place)	Logging and platform monitoring

A complete and updated list of sub-processors is available at opisense.com/subprocessors.

7.3 Sub-processor requirements

Opisense shall ensure that sub-processors:

- Are bound by confidentiality obligations at least as stringent as those in this DPA;
- Implement appropriate technical and organisational security measures;
- Comply with the principles of data protection law.

7.4 Changes to sub-processors

Opisense shall notify the Customer of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance by email to the Customer's registered contact address and by updating the Sub-processor Register at opisense.com/subprocessors. The Customer may object to the addition or replacement of a sub-processor on reasonable grounds relating to data protection by notifying Opisense in writing within 14 days of receiving the notification. If the Customer objects, the parties shall seek a mutually acceptable solution in good faith within 14 days of the objection. If no resolution is reached, Section 7.5 applies.

7.5 Customer objection

If the Customer objects to the appointment of a new sub-processor and the parties cannot reach agreement, the Customer may, as its sole and exclusive remedy, terminate the affected part of the Service without penalty upon written notice. This does not affect the Customer's obligations under any contract for already-processed data.

8. INTERNATIONAL DATA TRANSFERS

Personal data is primarily stored and processed within the EU/EEA on AWS infrastructure in Frankfurt, Germany.

Where sub-processors involve transfer of personal data to third countries, including OpenAI, Anthropic, Vercel, Convex, Ragie, Recall, Composio, Resend, Axiom, Elevenlabs, Stripe and Clerk, such transfers are conducted only on the basis of:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
- EU-US Data Privacy Framework, where applicable;
- Other adequate safeguards as permitted under GDPR Chapter V.

Opisense has conducted Transfer Impact Assessments (TIAs) for each sub-processor located outside the EU/EEA, evaluating the legal framework, government access practices, and supplementary measures in the receiving country. TIAs are reviewed annually and whenever material changes occur to the applicable legal framework or sub-processor arrangements. A summary of TIA conclusions is available upon written request to privacy@opisense.com.

A copy of the applicable SCCs is available on written request to contact@opisense.com.

Opisense shall resist data requests from foreign authorities that lack a valid legal basis under EU law, inform the Customer immediately upon receipt of any such request, and not grant access to personal data without the Customer's prior written consent or a legally binding order from a competent authority.

Where the Customer connects third-party services through the platform's integration capabilities, additional data transfers may occur in accordance with the terms of those third-party services. The Customer is responsible for ensuring that any third-party integrations comply with applicable data protection law.

9. ASSISTANCE TO THE DATA CONTROLLER

9.1 Data subject rights

Opisense shall, taking into account the nature of the processing, assist the Customer by appropriate technical and organisational means, in fulfilling the Customer's obligation to respond to data subject requests for access, rectification, erasure, restriction, portability, and objection in accordance with Chapter III of the GDPR.

9.2 Data protection impact assessment

Opisense shall assist the Customer in carrying out data protection impact assessments and prior consultations with supervisory authorities where required under Article 35 and 36 of the GDPR by providing all information necessary to demonstrate compliance with this DPA and applicable data protection law.

9.3 Personal Data Breach Notification

Opisense shall:

- Notify the Customer without undue delay and, where possible, within 24 hours of becoming aware of a personal data breach, to enable the Customer to meet its obligation to notify Datatilsynet within 72 hours under Article 33(1) of the GDPR;
- Provide, with the initial notification or as soon as reasonably practicable thereafter, a description of the breach including the nature and scope of the breach, the categories and approximate number of affected data subjects and personal data records, the likely consequences, and the measures taken or proposed to mitigate the effects;
- Assist the Customer in meeting its notification obligations under Article 33 and Article 34 of the GDPR, including providing all information necessary for the Customer to notify Datatilsynet and to communicate with affected data subjects where required;
- Document all personal data breaches, including the facts, effects, and remedial actions taken, and make this documentation available to the Customer upon request.

10. DELETION AND RETURN OF DATA

10.1 Customer choice upon termination

Following termination or expiration of the Service, the Customer may request that Opisense return all personal data in a commonly used and machine-readable format (e.g., JSON or CSV) or confirm the deletion of personal data. The Customer shall notify Opisense of its choice within 30 days of termination.

10.2 Retention after termination

Data type	Retention period
Voice data	7 days
Processed data	30 days then deleted
Other personal data	60 days
Legal retention data	Retained as required by law

10.3 Confirmation of deletion

Within 14 days of the deletion deadline, Opisense shall provide written confirmation to the Customer that all personal data has been deleted in accordance with this Section, unless a longer retention period is required by applicable law.

11. AUDIT AND DOCUMENTATION

11.1 Audit rights

The Customer may conduct at most one audit per calendar year to assess Opisense's compliance with this DPA. Additional audits may be conducted if a personal data breach occurs. Audits shall be conducted in accordance with Section 11.2.

11.2 Audit procedure

The Customer shall provide at least 14 days written notice before conducting an audit. Audits shall be conducted during normal business hours and in a manner that does not unreasonably interfere with Opisense's operations. Opisense may refuse to disclose information relating to other customers.

11.3 Documentation on request

Upon written request, Opisense shall provide the Customer with:

- Copies of its data protection and security policies;
- Relevant access logs and security event logs;
- Copies of Data Processing Agreements with its sub-processors;
- Reports of security testing and vulnerability assessments.

12. LIABILITY

The Customer, as the Data Controller, shall be liable to affected data subjects for any damage caused by processing that violates the GDPR, including losses and costs relating to notification and remediation, except where Opisense is responsible for the breach.

The Customer shall indemnify and hold harmless Opisense from any claims by data subjects arising from the Customer's breach of its obligations as Data Controller, including but not limited to collecting personal data without a valid legal basis, instructing Opisense to process personal data in violation of applicable law, or failing to obtain required consents from data subjects.

Opisense shall be liable for any damage caused by its processing activities that violate the GDPR, including breach of its obligations under this DPA, and shall indemnify and hold harmless the Customer from any such claims by data subjects.

Notwithstanding any limitations in the Master Services Agreement, Opisense's liability under this DPA shall be unlimited for: (i) unauthorised processing of personal data; and (ii) unlawful transfer of personal data to third countries.

For (iii) violations of data subject rights and (iv) breach of confidentiality, Opisense's liability shall be limited to the greater of three times the annual fees paid by the Customer in the 12 months preceding the claim, or EUR 250,000.

13. TERM AND TERMINATION

This DPA shall apply from the date the Customer starts using the Service and shall continue for as long as Opisense processes personal data on behalf of the Customer.

Upon termination or expiration of the underlying Service Agreement, Opisense's obligations under this DPA shall automatically terminate, except for the obligations in Sections 9, 10, and 11 which shall continue until all personal data has been deleted or returned. All parties shall comply with any post-termination obligations as set out in this DPA.

14. CHANGES TO THE DPA

Opisense may update this DPA from time to time to reflect changes in applicable law, regulatory guidance, or operational needs, provided that such changes do not materially weaken data protection safeguards. Opisense shall notify the Customer of any material changes and provide at least 30 days for review.

The Customer's continued use of the Service following notice of changes constitutes acceptance of the updated DPA. If the Customer does not accept the changes, the Customer may terminate the Service in accordance with the Master Services Agreement.

15. GOVERNING LAW AND JURISDICTION

This DPA shall be governed by and construed in accordance with Norwegian law, without regard to its conflict of law principles.

Complaints and administrative matters relating to data protection shall be subject to the jurisdiction of Datatilsynet (the Norwegian Data Protection Authority).

Civil disputes arising out of or relating exclusively to data protection matters under this DPA shall be subject to the exclusive jurisdiction of the Trondheim District Court.

For all other disputes relating to the commercial relationship between the parties, the dispute resolution provisions of the Master Services Agreement (or, where applicable, the Terms of Service) shall apply.

16. CONTACT

Contact details
Opisense AS
Organisation number: 936 578 195
Email: contact@opisense.com
Website: opisense.com

By using Opisense, the Customer accepts this Data Processing Agreement in its entirety. This DPA forms part of the agreement between the parties and supplements the Terms of Service.