Data Processing Agreement

Last updated: 9 June 2026

EXECUTIVE SUMMARY

This Data Processing Agreement (DPA) governs the processing of personal data by Opisense AS as a data processor on behalf of the Customer (data controller) under the Opisense Platform Service Agreement. The DPA implements Article 28 of the GDPR and aligns with EDPB Recommendations 01/2020 on Standard Contractual Clauses and Transfer Impact Assessments.

TABLE OF CONTENTS

1. DEFINITIONS AND INTERPRETATION

1.1 DEFINED TERMS

In this DPA, the following terms have the meanings set out below:

- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Processing" means any operation performed on Personal Data such as collection, recording, use, or erasure.
- "Data Subject" means the individual to whom Personal Data relates.
- "Controller" means the legal entity (Customer) determining the purposes and means of Processing.
- "Processor" means Opisense AS, engaged to Process Personal Data on behalf of the Controller.
- "Sub-processor" means an entity engaged by Opisense to Process Personal Data as a further processor.
- "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council.
- "SCC" means Standard Contractual Clauses approved by the European Commission.
- "DPF" means Data Privacy Framework, an adequacy mechanism for transfers to the United States.
- "TIA" means Transfer Impact Assessment, a documented assessment of data transfer risks per Schrems II.

2. SCOPE OF PROCESSING

2.1 CUSTOMER INSTRUCTIONS

Opisense processes Personal Data solely on documented instructions from the Customer and as necessary to provide the Opisense Platform Service. Processing instructions are set out in the Platform Service Agreement and this DPA.

2.2 PROCESSING ACTIVITIES

Opisense engages in the following Processing activities on behalf of the Customer:

- Collection: Ingestion of customer data via Platform API and user uploads
- Storage: Persistent storage in Hetzner (EU) and Supabase / Convex data backends
- Analysis: Processing via LLM models (OpenAI, Anthropic) for inference and feature delivery
- Enhancement: Voice synthesis (Elevenlabs), document processing (Recall), agent web browsing (Browserbase), code execution (Daytona)
- Use: Delivering personalized recommendations, automated workflows, and analytics
- Deletion: Erasure of Personal Data upon Customer request or Service termination

3. PROCESSING INSTRUCTIONS

3.1 AUTHORIZATION

The Customer authorizes Opisense to Process Personal Data in accordance with the Service Agreement, this DPA, and documented written instructions from the Customer. The Customer may issue additional Processing instructions in writing; Opisense shall implement reasonable instructions without undue delay and in a manner consistent with the Service Agreement.

3.2 RESTRICTIONS ON PROCESSING

Opisense shall not Process Personal Data for purposes other than those authorized by the Customer, except as required by applicable law. Opisense shall not disclose Personal Data to any third party except:

- Sub-processors authorized under Section 7 of this DPA
- Law enforcement or regulatory authorities with valid legal process
- In response to data subject rights requests as instructed by the Customer

4. SECURITY AND ORGANIZATIONAL MEASURES

4.1 TECHNICAL AND ORGANIZATIONAL MEASURES

Opisense implements appropriate technical and organizational measures appropriate to the risk and state of the art, in accordance with Article 32 of the GDPR. These measures include:

- Encryption: TLS 1.2+ in transit; AES-256 at rest for Personal Data
- Access Control: Role-based access control (RBAC); multi-factor authentication (MFA) required
- Availability: Redundant infrastructure across Hetzner data centres and availability zones; automated backup and recovery
- Confidentiality: Data minimization; strict access logging and monitoring
- Regular Reviews: Annual security audits by independent third parties; penetration testing

4.2 VULNERABILITY MANAGEMENT

Opisense maintains a documented vulnerability management program:

- Quarterly vulnerability scanning and remediation of identified issues
- External Penetration Testing: Independent external security firm conducts comprehensive penetration testing at least annually

5. DATA RETENTION AND DELETION

5.1 RETENTION PERIOD

Opisense retains Personal Data for as long as necessary to provide the Service, unless a longer retention period is required by law. Upon Customer request or at Service termination, Opisense shall delete or return Personal Data within 30 days.

5.2 DELETION CERTIFICATION

Opisense provides written certification of data deletion upon Customer request, confirming deletion from all systems including backups within the retention period.

6. DATA SUBJECT RIGHTS

6.1 SUPPORT FOR DATA SUBJECT REQUESTS

Opisense shall, taking into account the nature of Processing, assist the Customer by appropriate technical and organizational measures to fulfill data subject rights under Articles 15–22 of the GDPR (access, rectification, erasure, restriction, portability, objection, and automated decision-making).

6.2 RESPONSE TIMELINE

Opisense shall respond to Customer requests for assistance with data subject rights within 10 business days. For complex requests, Opisense shall provide a timeline and interim updates.

7. SUB-PROCESSORS

7.1 GENERAL AUTHORIZATION

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

7.2 CURRENT SUB-PROCESSORS

Current sub-processors are listed at opisense.com/legal/subprocessor-register-opisense and include infrastructure, AI inference, storage, and monitoring providers. Primary sub-processor categories:

- Cloud infrastructure: Hetzner (EU), Vercel
- AI providers: OpenAI, Anthropic (LLM inference) routed via the OpenRouter gateway
- Data processing: Recall (document processing), Elevenlabs (voice synthesis), Browserbase (agent browsing), Daytona (code execution)
- Storage and database: Convex, Supabase, Hetzner
- Monitoring and observability: Axiom
- Other services: Clerk (authentication), Stripe and Mollie (payments), Resend (email)

7.3 SUB-PROCESSOR REQUIREMENTS

All sub-processors are bound by data processing agreements that incorporate Article 28 obligations and standards at least as stringent as this DPA. Specific requirements include:

- **Written Data Processing Agreements:** Each sub-processor executes a written Data Processing Agreement (or Standard Contractual Clauses where applicable) that includes the commitments required by this Section.
- **International Transfer Mechanisms:** For sub-processors located outside the European Economic Area, Opisense implements measures designed to compliance with GDPR Chapter V (International Transfers) via Data Privacy Framework or Standard Contractual Clauses, as documented in Transfer Impact Assessments.
- **Sub-processor Review:** Sub-processor Data Processing Agreements and transfer mechanism documentation are reviewed annually. Changes to sub-processors or transfer mechanisms are documented and tracked in the Sub-processor Register (LEGAL-SUBPROC-001).
- **Right to Object:** The Customer may object to engagement of a new sub-processor within 30 days of notification. Unresolvable objections entitle the Customer to terminate the affected Service.

7.4 SUB-PROCESSOR CHANGES

Opisense will notify the Customer at least 30 days in advance of any new sub-processor or material change to a sub-processor's role or country of processing. Notification shall be made via email to the Customer's designated contact and shall include the sub-processor's name, country, and role in Service delivery.

8. INTERNATIONAL DATA TRANSFERS

8.1 PRIMARY PROCESSING LOCATION

Opisense processes personal data in the European Union (Hetzner data centres in Germany and Finland) as the primary processing location. EU-based sub-processors (Hetzner, Mollie) involve no third-country transfer. Certain processing activities (AI inference, specialized services) require engagement of US-based sub-processors to deliver Service features, for which the transfer mechanisms in Section 8.2 apply.

8.2 SUB-PROCESSOR TRANSFER DOCUMENTATION

The following sub-processors engage in international data transfers:

- OpenAI (US): SCC + TIA completed (ref. TIA-LEGAL-003)
- Anthropic (US): SCC + TIA completed (ref. TIA-LEGAL-003)
- Elevenlabs (US): DPF + SCC + TIA completed (ref. TIA-LEGAL-002)
- Supabase (US): SCC + TIA completed; EU region (Frankfurt) (ref. TIA-LEGAL-004)
- Recall (US): DPF + SCC + TIA completed (ref. TIA-LEGAL-005)
- Composio (US): SCC + TIA completed (ref. TIA-LEGAL-005)
- Vercel (US): DPF + SCC + TIA completed (ref. TIA-LEGAL-002)
- Clerk (US): DPF + SCC + TIA completed (ref. TIA-LEGAL-002)
- Stripe (US): DPF + SCC + TIA completed (ref. TIA-LEGAL-002)
- Resend (US): DPF + SCC + TIA completed (ref. TIA-LEGAL-002)
- Axiom (US): SCC + TIA completed (ref. TIA-LEGAL-004)
- Convex (US): SCC + TIA completed (ref. TIA-LEGAL-004)
- OpenRouter (US): SCC + TIA completed; EU in-region routing enabled (ref. TIA-LEGAL-003)
- Browserbase (US): SCC + supplementary measures + TIA completed (ref. TIA-LEGAL-005)
- Daytona (US): SCC + TIA completed (ref. TIA-LEGAL-005)

Detailed Transfer Impact Assessments are documented in TIA-LEGAL-001 through TIA-LEGAL-005, covering the US legal regime assessment, all processor-specific risk analyses, and supplementary measures. These assessments are conducted in accordance with EDPB Recommendations 01/2020 and the CNIL practical guide on TIAs, and are reviewed quarterly. Complete TIA documentation is available for Customer review upon request.

Customers concerned about specific sub-processors or transfer mechanisms may contact the DPO at dpo@opisense.com for additional documentation or discussion of alternative arrangements.

8.3 STANDARD CONTRACTUAL CLAUSES

Opisense has executed EU Commission-approved Standard Contractual Clauses (Module Two: Controller to Processor; Module Three: Processor to Processor) with all sub-processors located outside the EEA, in accordance with the European Commission Decision 2021/915.

8.4 DATA PRIVACY FRAMEWORK

US-based sub-processors holding valid Data Privacy Framework certifications are regularly verified for active DPF enrollment. DPF adequacy monitoring is conducted quarterly per Section 4.4 of the Sub-processor Register.

8.5 SUPPLEMENTARY MEASURES

Where Standard Contractual Clauses alone are insufficient to address identified risks from third-country legislation (e.g., FISA, Executive Order 12333), Opisense implements supplementary measures as documented in Transfer Impact Assessments, including:

- Data minimization at source (limiting transmission to necessary data only)
- Encryption and pseudonymization where feasible
- Contractual commitments for non-disclosure and protective measures
- Regular monitoring and re-assessment of adequacy

9. AUDIT AND COMPLIANCE

9.1 CUSTOMER AUDIT RIGHTS

The Customer retains the right to audit Opisense's processing of Personal Data, either directly or via a qualified independent auditor, during business hours with reasonable notice (at least 15 business days). Audits shall be conducted no more frequently than once per calendar year unless there is reasonable grounds for concern.

9.2 AUDIT COOPERATION

Opisense shall cooperate fully with audit activities, including providing access to systems, personnel, documentation, and security certifications (SOC 2, ISO 27001). Confidential information shall be subject to protective agreements.

9.3 REGULATORY AUDITS

Opisense shall notify the Customer promptly upon receipt of any audit notice, data protection investigation, or regulatory inquiry that may affect Processing of the Customer's Personal Data, except where legally prohibited.

10. DATA BREACH NOTIFICATION

10.1 BREACH NOTIFICATION OBLIGATION

Opisense shall notify the Customer without undue delay after becoming aware of a confirmed or reasonably suspected personal data breach affecting the Customer's Personal Data.

10.2 NOTIFICATION CONTENT

Breach notification shall include:

- Nature and scope of the breach (data categories, approximate number of data subjects)
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate harm
- Contact information for further inquiries

10.3 COOPERATION WITH AUTHORITIES

Opisense shall cooperate with the Customer and data protection authorities in investigation and remediation of breaches, including preservation of evidence and provision of forensic reports.

11. TERM AND DELETION OF PERSONAL DATA

11.1 RETENTION PERIOD

Opisense retains Personal Data for as long as necessary to provide the Service, unless a longer retention period is required by law. On termination of the Service Agreement, or on Customer request, the Customer may export or retrieve its Personal Data within 30 days, after which Opisense deletes or returns the data in accordance with Section 11.3.

11.2 DELETION CERTIFICATION

Opisense provides written certification of deletion, confirming that Personal Data has been deleted from all systems, backups, and archives in accordance with Opisense's retention and destruction policies.

11.3 POST-TERMINATION DELETION

Following the 30-day export window described in Section 11.1, Opisense shall, at the Customer's option, delete or return all Personal Data and complete deletion from all production systems, backups, and archives within 60 days of termination of the Service Agreement or Customer request, unless a longer retention period is required by applicable law. Backup media are deleted as they are cycled and overwritten within this period.

12. LIABILITY AND INDEMNIFICATION

12.1 PROCESSOR LIABILITY

Opisense's liability for Processing of Personal Data is limited as set out in the Platform Service Agreement. Opisense shall not be liable for Customer's failure to comply with GDPR obligations as data controller, including failure to comply with data subject rights requests, obtain valid legal basis for Processing, or maintain required records.

12.2 INDEMNIFICATION

Each party shall indemnify the other from third-party claims arising from its own material breach of this DPA. Opisense shall indemnify the Customer for claims arising from Opisense's breach of its data processor obligations under Chapter III of GDPR (Articles 28-36).

SIGNATURE

This Data Processing Agreement is entered into effective as of the date first signed for use of Opisense.