

Master Services Agreement

Last updated: 9 June 2026



This Master Services Agreement governs the relationship between Opisense AS and the Customer for use of the Opisense platform. Governed by Norwegian law, intended for business customers. Read alongside the Data Processing Agreement, Privacy Notice, AI Policy, and Acceptable Use Policy at opisense.com/legal.

1. DEFINITIONS

This Master Services Agreement governs the relationship between Opisense AS and the Customer for use of the Opisense platform.

2. SCOPE AND DOCUMENT HIERARCHY

2.1 WHAT THIS AGREEMENT COVERS

This Agreement governs Opisense delivery of the Service as Software as a Service and the Customer use of the Service.

2.2 DOCUMENT HIERARCHY

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

- (i) Service Order Form or service specification
- (ii) Data Processing Agreement
- (iii) This Master Services Agreement
- (iv) Terms of Service
- (v) Acceptable Use Policy and AI Policy

2.3 ACCEPTANCE

This Agreement is binding from the moment the Customer actively confirms acceptance during platform registration or by signing a written agreement with Opisense. Passive use does not constitute acceptance.

3. SERVICE DELIVERY AND AVAILABILITY

3.1 SERVICE DESCRIPTION

Opisense provides an AI-powered business platform that combines an intelligent workspace, AI agents, automation, and an integration and security layer to support companies in running and improving their daily operations.

The platform includes, and may be extended to include, functional modules and capabilities spanning areas such as knowledge management, meeting and collaboration tools, content creation, planning, analytics, HR, finance, production, logistics, and other operational domains. The specific modules and features available to the Customer depend on the subscription plan, service configuration, and platform version at the time of use. The Service is available at opisense.com and workspace.opisense.com.

3.2 UPTIME

Opisense commits to maintain 99.5% uptime per calendar month, measured in accordance with the Service Level Agreement, excluding planned maintenance communicated with 48 hours notice. If actual uptime falls below the target for two or more consecutive months, Customer may elect: (a) service credits as specified in the SLA, or (b) termination without penalty. Uptime and incident management are governed by the Service Level Agreement.



3.3 MAINTENANCE

Planned maintenance is communicated at least 48 hours in advance and scheduled to minimise disruption. Emergency maintenance may occur without prior notice in the event of security threats or critical failures.

Opisense is not liable for downtime caused by force majeure events beyond the reasonable control of either party, including natural disasters, power outages, governmental orders, or pandemics. However, force majeure does not relieve Opisense or the Customer of their obligations under the Data Processing Agreement or applicable data protection laws, including GDPR requirements for security, breach notification, or data subject rights. Specifically:

- During a force majeure event, Opisense continues to apply security measures appropriate to the circumstances in accordance with GDPR Article 32 and to fulfil breach notification obligations under GDPR Article 33 to the extent reasonably practicable.
- If a force majeure event impacts a third-party sub-processor, Opisense shall use commercially reasonable efforts to notify the Customer promptly and activate applicable recovery procedures. Opisense's responsibility is limited to: (a) demonstrating that sub-processors were selected based on documented evaluation criteria, and (b) maintaining oversight of sub-processor data protection practices. Opisense is not liable for sub-processor failures or performance degradation resulting from force majeure events. Liability for personal data breaches arising from such events is determined in accordance with GDPR Article 82 and the liability provisions of this Agreement.
- The Customer's data protection rights (Articles 15-22, GDPR) remain applicable during force majeure events. Response timelines under GDPR are extended to the extent the force majeure event makes timely compliance impracticable, in accordance with supervisory authority guidance.

If a force majeure event prevents either party from performing its obligations for a period exceeding 30 days, either party may terminate the affected Service component(s) without penalty on written notice.

4. CUSTOMER ACCESS AND USE

4.1 LICENCE

Opisense grants the Customer a non-exclusive, non-transferable, time-limited licence to use the Service for the duration of this Agreement, in accordance with the Acceptable Use Policy and the terms herein.

4.2 USER ACCESS

The Customer may authorise Users to access the Service. The Customer is responsible for User actions and compliance with this Agreement. Users must keep login credentials confidential and notify Opisense immediately of any suspected unauthorised access.

Master Services Agreement

Last updated: 9 June 2026



4.3 PROHIBITED USE AND DATA MINIMISATION

The Customer and Users shall not:

- Use the Service for unlawful purposes or in breach of local or international law
- Attempt unauthorised access to the Platform or any of its systems
- Transmit harmful code, viruses, malware, or other malicious content
- Reverse-engineer, decompile, or modify the Service or its components
- Resell, redistribute, or sublicense access to the Service without written approval
- Use the Service to process personal data in violation of GDPR Article 5 (principles)

Specifically regarding personal data processing (GDPR Article 5(1)(b)):

- **Data Minimisation Principle:** Customers shall only submit personal data that is necessary and relevant for the specific service purpose. Opisense recommends that Customers apply data minimisation practices, including:
 - De-identifying or anonymizing personal data before upload where practically possible
 - Excluding unnecessary personal data categories (e.g., full home addresses when only location is needed)
 - Limiting the scope and duration of personal data retention within the platform
- **Customer Responsibility:** The Customer remains solely responsible for ensuring it has a valid lawful basis (GDPR Article 6) and appropriate legal justification for processing any personal data submitted to Opisense. Opisense acts as data processor and implements technical safeguards but does not independently evaluate the Customer's legal basis.
- Circumvent security measures or usage restrictions

Full details on acceptable use are set out in the Acceptable Use Policy at opisense.com/legal.

5. PRICING AND PAYMENT

5.1 PRICING STRUCTURE

The Service is priced on two components:

- Subscription component: Fixed monthly or annual fee per User or organisation
- Usage-based component: Variable cost based on actual use (recordings, transcriptions, AI processing, or other measurable activities)

Specific prices are set out in the Customer's order confirmation or public price list at opisense.com.

5.2 INVOICING AND PAYMENT

Invoicing occurs monthly or annually as agreed. Usage-based costs are invoiced in arrears based on consumption in the previous billing period. Payment is due 14 days from the invoice date. In the event of late payment beyond 14 days, Opisense may suspend access to the Service and charge late payment interest in accordance with the Norwegian Late Payment Interest Act.

5.3 VAT

All prices are stated exclusive of value added tax (VAT). Applicable VAT will be added to invoices in accordance with Norwegian law.

5.4 PRICE CHANGES

Opisense may adjust prices with 60 days written notice by email. Existing annual subscriptions are not affected until the next renewal date. Annual price increases shall not exceed 7.5%. For Material changes, the Customer may terminate without penalty by written notice within 10 business days.



6. INTELLECTUAL PROPERTY

6.1 OPISENSE RIGHTS

Opisense owns all rights, title, and interest in the Platform and underlying technology, including the platform architecture, AI models and algorithms, documentation, and trademarks.

6.2 CUSTOMER DATA

The Customer retains all rights to data uploaded or submitted to the platform, output generated from their input, and metadata associated with their use. Opisense makes no claim to ownership of Customer Data and will not use Customer Data to train AI models without explicit written consent.

6.3 LICENCE TO PROCESS CUSTOMER DATA

The Customer grants Opisense a worldwide, non-exclusive, irrevocable licence (for the duration of this Agreement) to process Customer Data to the extent necessary to deliver the Service. The licence automatically expires on termination of this Agreement, except for data retained in accordance with applicable law or the Data Processing Agreement.

7. DATA PROTECTION AND SECURITY

7.1 DATA PROCESSING AGREEMENT

Processing of personal data and other sensitive data is governed by the Data Processing Agreement (DPA) at opisense.com/legal, which forms part of this Agreement. The DPA incorporates security, encryption, audit, and sub-processor provisions required under GDPR, NIS2, and applicable Norwegian law.

7.2 SECURITY STANDARDS

Opisense maintains a comprehensive information security management system (ISMS) aligned with ISO 27001:2022. Key commitments include:

- Data encryption: AES-256 for data at rest; TLS 1.2 minimum for data in transit (EU region — Germany and Finland)
- Access control: Authentication, authorisation, and role-based access control (RBAC)
- Vulnerability management: Critical vulnerabilities patched within 72 hours of patch availability; high-severity within 7 days
- Incident response: 48-hour customer notification of personal data breaches; 72-hour notification to Data Protection Authority as required
- Audit and monitoring: Continuous security monitoring, planned annual penetration testing, and third-party audits

Detailed security measures are documented in the DPA and Opisense Security Standards.

7.3 SUB-PROCESSORS

Opisense uses third-party sub-processors to deliver the Service. Current sub-processors are listed at opisense.com/legal/subprocessor-register-opisense. Opisense will notify Customers of any new sub-processor or changes to existing sub-processors at least 30 days in advance. Customers may object to new sub-processors by providing written notice to contact@opisense.com within 15 days; if unresolved, the Customer may terminate the affected Service component without penalty.

7.4 RISK APPETITE AND RESIDUAL RISK

Opisense operates under a defined risk appetite framework whereby residual risk is maintained within organisational tolerance levels across all material information security domains. Risk assessments are conducted at least annually and following any Material changes to the platform.



8. CONFIDENTIALITY

8.1 CONFIDENTIAL INFORMATION

Each party acknowledges that it may receive confidential information from the other party. Confidential information includes the terms of this Agreement, technical details, Customer Data, and other non-public information marked as confidential or that reasonably appears to be confidential.

8.2 OBLIGATIONS

Each party agrees to:

- Keep confidential information strictly confidential
- Use confidential information solely to perform its obligations or exercise its rights under this Agreement
- Protect confidential information with the same level of care it uses to protect its own confidential information, but no less than reasonable care
- Limit access to confidential information to employees and contractors with a need to know

8.3 EXCEPTIONS

Confidentiality obligations do not apply to information that: (a) is or becomes public through no breach of this Agreement; (b) is rightfully received from a third party without confidentiality restrictions; (c) is independently developed without reference to the other party's information; or (d) must be disclosed by law or regulatory order, provided the disclosing party gives prompt notice to allow the other party to seek protective measures.

9. LIMITATIONS OF LIABILITY

9.1 EXCLUDED DAMAGES

Except in cases of gross negligence or wilful misconduct, neither party is liable to the other for indirect, incidental, consequential, special, or punitive damages, including lost profit, lost revenue, lost data (where the Customer has maintained backups), business interruption, or reputational harm.

9.2 CAP ON LIABILITY

Each party's total aggregate liability to the other party shall not exceed the fees paid or payable by the Customer under this Agreement in the 12 months preceding the claim. This cap does NOT apply to:

- Liability for GDPR violations, data protection breaches, or breach of data subject rights
- Liability for Opisense's failure to implement or maintain security measures required under the Data Processing Agreement
- Liability for personal data breaches or unauthorized disclosure of personal data
- Liability for infringement of intellectual property rights
- Gross negligence or wilful misconduct
- Indemnification obligations
- Termination consequences under Section 14.4

9.3 SPECIFIC EXCLUSIONS

Opisense is not liable for:

- Claims arising from Customer Data or input submitted by the Customer
- Personal data breaches caused by Opisense's failure to implement required security measures (as documented in the DPA) - for such breaches, Opisense's liability is unlimited per Section 9.2
- Claims arising from Opisense infringement of Customer intellectual property rights

Master Services Agreement

Last updated: 9 June 2026



9.4 INDIRECT LOSSES

Opisense is not liable for indirect losses, including lost profit, reputational damage, loss of opportunities, data loss where the Customer has not maintained backups, or loss resulting from inaccuracy in AI-generated content.

10. TERM AND TERMINATION

10.1 TERM

This Agreement commences when the Customer accepts the terms (Section 2.3) and continues for the duration of the paid subscription or as otherwise agreed.

10.2 TERMINATION FOR CONVENIENCE

The Customer may terminate this Agreement at the end of any subscription period by providing 30 days written notice. Termination for convenience during an annual subscription period may trigger early termination fees as set out in the Service Order.

10.3 TERMINATION FOR CAUSE

Either party may terminate this Agreement immediately upon written notice if:

- The other party materially breaches this Agreement and fails to cure the breach within 30 days of receiving written notice of the breach
- The other party becomes insolvent or enters liquidation
- The other party ceases to conduct business

10.4 EFFECT OF TERMINATION

Upon termination or expiration:

- The Customer's licence to use the Service immediately terminates
- The Customer remains responsible for all fees accrued through the termination date
- Opisense shall delete or return Customer Data in accordance with the Data Processing Agreement (Section 11)
- Provisions that by their terms survive termination (confidentiality, limitation of liability, data protection, IP rights) shall remain in effect

SIGNATURE

By registering for or using the Opisense platform, the Customer agrees to and accepts the terms of this Master Services Agreement.

Opisense AS
Org.nr. 936 578 195
contact@opisense.com
www.opisense.com