Privacy Notice

Last updated: 9 June 2026

INTRODUCTION

This Privacy Notice explains how Opisense AS ("Opisense", "we", "us") collects, uses, stores and protects personal data in connection with the Opisense AI-powered business platform and our websites. It applies to website visitors, platform users, customers and business contacts.

This notice is prepared in accordance with GDPR Articles 13 and 14, the Norwegian Personal Data Act, and the Norwegian Electronic Communications Act.

1. DATA CONTROLLER

Opisense AS is the data controller for the personal data processed in connection with our platform and websites.

For business customers, Opisense may act as a Data Processor, processing personal data on your behalf according to a separate Data Processing Agreement.

2. WHAT DATA WE COLLECT AND WHY

2.1 WEBSITE VISITORS

Opisense does not use website analytics or third-party tracking technologies, and does not collect personal data from website visitors for analytics purposes.

2.2 CONTACT ENQUIRIES

When you contact us with an enquiry, we collect your name, email address, phone number, and message content. Legal basis: Legitimate interest. Retention: 24 months after last contact.

2.3 PLATFORM USERS

For platform users, we collect: user account information (name, email, profile data), input data (documents, text, files you upload), output data (results generated by the platform), activity data (actions taken in the platform), technical data (device info, browser, IP address), and integration data (connected services and authentication credentials). Legal basis: Contractual necessity.

DATA CATEGORIES – DETAILED DEFINITIONS

Input Data means any text, files, or media submitted by the user to the AI agent. This includes prompts, documents, images, spreadsheets, emails, and other user-provided content used to generate outputs or train models.

Activity Data means interaction logs, timestamps, feature usage patterns, button clicks, API calls, session duration, login/logout events, and other telemetry collected to understand how users interact with the Opisense platform. Activity data does not include the content of input or output data.

2.4 CUSTOMERS AND BUSINESS CONTACTS

For customers and business contacts, we collect name, email, phone number, billing address, payment information, and communication records. Legal basis: Contractual necessity and legitimate interest.

3. LEGAL BASES FOR PROCESSING

Opisense processes personal data only where a lawful basis under GDPR Article 6 applies. The legal basis for each processing activity is as follows:

- Responding to contact enquiries (name, email, phone, message content): legitimate interest — Article 6(1)(f).
- Providing the platform and delivering the service to users (account, input, output, activity, technical and integration data): performance of a contract — Article 6(1)(b).
- Account administration and customer relationship management (customer and business-contact details and communication records): performance of a contract — Article 6(1)(b), and legitimate interest — Article 6(1)(f).
- Billing, payments and statutory accounting records (billing address, payment information, invoices): legal obligation — Article 6(1)(c) (Norwegian Bookkeeping Act), and performance of a contract — Article 6(1)(b).
- Security, monitoring, logging and fraud prevention (technical and activity data, security logs): legitimate interest — Article 6(1)(f).
- Compliance with legal obligations and responding to lawful requests from public authorities: legal obligation — Article 6(1)(c).

4. RETENTION PERIODS

Opisense retains personal data only for as long as necessary for the purposes for which it was collected, unless a longer period is required by law. Retention periods by category are:

- Contact enquiry data: 24 months after last contact.
- Platform user account and content data (input, output, activity, technical and integration data): for the duration of the user account and the service agreement. On account closure, service termination, or Customer request, you may export or retrieve this data within 30 days; Opisense then deletes or returns all remaining data, including from backups, within 60 days, in accordance with our Data Processing Agreement (Section 11.3).
- Customer and business-contact data: for the duration of the business relationship, then deleted within 60 days, unless a longer statutory retention period applies.
- Billing, payment and accounting records: retained for 5 years from the end of the relevant accounting year, as required by the Norwegian Bookkeeping Act.
- Security and system logs: retained only for as long as necessary for security, audit and fraud-prevention purposes, the criteria being the relevant security, legal and operational needs, after which they are deleted.
- Backups: deleted on a rolling cycle, with backup copies removed within 30 days.

5. SHARING OF PERSONAL DATA

We do not sell your personal data. Personal data is shared only with:

- Sub-processors: Third-party service providers who process data on our behalf to deliver the Opisense platform (see Section 6).
- Public authorities: When legally required by court order, law enforcement, or regulatory authorities.
- Acquiring entities: In case of merger, acquisition, or business transfer, personal data may be transferred to the acquiring entity under the same privacy terms.

6. SUB-PROCESSORS

We engage sub-processors across the following categories to deliver the platform: cloud infrastructure and hosting (located in the European Union); application platform, database and storage; AI model inference and gateway services; specialised AI features including voice synthesis, document processing, agent web browsing and code execution; authentication, payments and transactional email; and monitoring and observability. Our primary hosting and data storage are located in the European Union.

An updated list of sub-processors is available at opisense.com/legal/subprocessor-register-opisense. Customers are notified at least 30 days before new sub-processors are engaged.

7. INTERNATIONAL DATA TRANSFERS

Personal data is primarily processed and stored within the EU/EEA, with primary hosting located in the European Union (data centres in Germany and Finland). Where data is transferred to countries outside the EU/EEA (such as the USA) for specific AI inference or specialised services, we rely on European Commission-approved Standard Contractual Clauses (SCCs) and, where the provider is certified, the EU-US Data Privacy Framework (DPF), each supported by a Transfer Impact Assessment. The full list of sub-processors and their applicable transfer mechanisms is maintained in our Sub-processor Register at opisense.com/legal/subprocessor-register-opisense. You may obtain details of the transfer mechanisms in place by contacting us.

8. COOKIES

Our website uses cookies for functionality only (essential and preference cookies). We do not use analytics or marketing cookies. Please refer to our Cookie Notice at opisense.com/legal/cookie-notice-opisense for full details.

9. SECURITY

We implement appropriate technical and organisational measures to protect personal data, including:

- TLS 1.3 encryption for all data in transit
- AES-256 encryption for data at rest
- Role-based access control (RBAC) and least privilege principles
- Multi-factor authentication (MFA) for all staff and users where feasible
- Continuous security monitoring and logging
- Regular security assessments and penetration testing where appropriate to risk profile and technical architecture
- Staff data protection and security training

10. PERSONAL DATA BREACHES

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, we will notify the Norwegian data protection authority (Datatilsynet) within 72 hours of becoming aware of it. Where required by law, we will also notify affected individuals without undue delay.

11. AUTOMATED DECISION-MAKING

We do not make fully automated decisions about you that have legal or similarly significant effects. The AI agents feature operates as a support tool to assist users with decision-making, but final decisions remain with the user.

12. CHILDREN

Our services are not directed at children under the age of 18. We do not knowingly collect personal data from children. If we become aware that we have collected data from a child, we will delete it promptly.

13. YOUR RIGHTS

Under GDPR and Norwegian data protection law, you have the following rights:

RIGHT TO OBJECT

Right to object to direct marketing: You have the unconditional right to object to processing of your personal data for direct marketing purposes (including newsletters and promotional communications) at any time.

Right to object to legitimate interests processing: You have the right to object to processing based on our legitimate interests (e.g., fraud prevention, account security) on grounds relating to your particular situation.

To exercise any of these rights, contact us at contact@opisense.com. We will respond within 30 days of your request.

14. RIGHT TO COMPLAIN

You have the right to lodge a complaint with the Norwegian data protection authority:

15. REGULATORY REFERENCES

This Privacy Notice is prepared in accordance with:

- Regulation (EU) 2016/679 (General Data Protection Regulation — GDPR)
- Norwegian Personal Data Act of 15 June 2018
- Norwegian Electronic Communications Act
- Network and Information Security Directive 2 (NIS2) — EU Directive 2022/2555 (where applicable to our security and incident reporting practices)

16. CHANGES TO THIS NOTICE

We may update this Privacy Notice from time to time to reflect changes in our practices or legal requirements. We will notify you by email and update the date at the top of this notice. Your continued use of our services after changes constitute your acceptance of the updated Notice.

17. CONTACT

If you have any questions or concerns about this Privacy Notice or how we process your personal data, please contact us:

DATA PROTECTION OFFICER

Email: dpo@opisense.com

We encourage you to contact us with any questions about how we handle your personal data.