Code of Conduct

Last updated: 9 June 2026

Organisation number: 936 578 195 | contact@opisense.com

This Code of Conduct establishes the ethical principles, professional standards, and governance commitments that guide Opisense AS in its operations, product development, and interactions with customers, partners, regulators, and the public. It applies to all persons acting on behalf of Opisense, including founders, employees, contractors, and agents. This document should be read alongside the AI Policy, Data Processing Agreement, Acceptable Use Policy, and other governance documents available at opisense.com/legal.

1. PURPOSE AND SCOPE

1.1 PURPOSE

Opisense builds AI-powered tools that companies use to run their operations. The data our customers entrust to us, and the decisions our AI systems help inform, carry real consequences. This Code of Conduct exists to ensure that every person at Opisense understands and upholds the standards required to be worthy of that trust.

1.2 SCOPE

This Code applies to all founders, employees, contractors, consultants, and any other individuals performing work on behalf of Opisense AS, regardless of role, seniority, or location. It also applies to all business activities, including product development, sales, customer support, partnerships, and public communications.

1.3 ACCOUNTABILITY

The CEO of Opisense AS is ultimately accountable for the implementation and enforcement of this Code. All persons covered by this Code are individually responsible for understanding and complying with its provisions. Violations are subject to disciplinary action, up to and including termination of employment or engagement.

2. DATA PROTECTION AND PRIVACY

Customer data is the foundation of the trust relationship between Opisense and its customers. Opisense commits to the following principles:

- Customer data is processed solely for the purposes defined in the Data Processing Agreement and in accordance with the customer's documented instructions.
- Customer data is never used to train, fine-tune, or improve AI models without the customer's explicit written consent.
- Personal data is handled in accordance with GDPR, the Norwegian Personal Data Act, and all applicable data protection legislation.
- Access to customer data is restricted to personnel who require it to perform their duties, and is logged and auditable.
- Data breaches are reported to affected customers within 48 hours and to Datatilsynet within 72 hours, in accordance with GDPR Article 33 and the Data Processing Agreement.
- Data minimisation, storage limitation, and purpose limitation principles are applied to all processing activities.

Every person at Opisense receives data protection training upon joining and annually thereafter. The data protection contact can be reached at dpo@opisense.com.

3. RESPONSIBLE AI

Opisense develops and deploys AI systems that support human decision-making. Our AI governance commitments are:

3.1 TRANSPARENCY

- AI-generated content is clearly identified as such within the platform.
- Customers and users are informed when they are interacting with AI features.
- Technical documentation for AI systems is maintained and available to customers and regulators upon request.

3.2 HUMAN OVERSIGHT

- AI systems operate as decision-support tools. Final decisions of consequence remain with humans.
- Users retain the ability to review, modify, or reject AI-generated outputs at all times.
- High-impact actions by AI agents include human-review checkpoints.

3.3 FAIRNESS AND NON-DISCRIMINATION

- Opisense monitors AI outputs for bias, discrimination, and harmful patterns.
- Customers are prohibited from using the platform for social scoring, biometric categorisation, subliminal manipulation, or any other use classified as unacceptable risk under Article 5 of the EU AI Act.
- Opisense does not develop or deploy AI systems intended to exploit the vulnerabilities of specific groups.

3.4 AI LITERACY

In accordance with Article 4 of the EU AI Act, Opisense implements measures to ensure that all personnel involved in the development, deployment, and support of AI features receive training on AI capabilities, limitations, risks, and responsibilities. Customers are expected to provide equivalent training to their users, as set out in the AI Policy.

4. INFORMATION SECURITY

Opisense maintains an Information Security Management System in accordance with

ISO 27001:2022. All personnel are bound by the following security obligations:

- Confidential information, including customer data, business secrets, and internal communications, must be protected at all times.
- Access credentials must not be shared. Multi-factor authentication is required for all administrative and staff accounts.
- Devices used for work must be encrypted and protected by strong authentication.
- Security incidents, suspected breaches, and vulnerabilities must be reported immediately to the security team at security@opisense.com.
- Information assets are classified and handled according to their classification level.

Security awareness training is provided to all personnel upon joining and annually thereafter.

5. ANTI-CORRUPTION AND ETHICAL BUSINESS PRACTICES

5.1 ANTI-CORRUPTION

Opisense has a strict policy against corruption, bribery, and facilitation payments, with all reported incidents subject to investigation and appropriate action in any form. No person acting on behalf of Opisense may offer, promise, give, request, or accept any bribe, kickback, or improper payment to or from any person, whether in the public or private sector. This applies regardless of local business customs or competitive pressure.

5.2 GIFTS AND HOSPITALITY

Modest gifts and reasonable business hospitality may be offered or accepted where they are lawful, transparent, proportionate, and would not create an actual or perceived conflict of interest. Any gift or hospitality exceeding NOK 1,000 in value must be disclosed to the CEO in advance.

5.3 CONFLICTS OF INTEREST

All personnel must avoid situations where personal interests conflict, or could reasonably appear to conflict, with Opisense's interests. Potential conflicts must be disclosed to the CEO promptly. This includes financial interests in competitors, customers, or suppliers, secondary employment or consultancy arrangements that overlap with Opisense's business, and personal relationships with individuals at organisations Opisense does business with.

5.4 FAIR COMPETITION

Opisense competes fairly and in compliance with applicable competition and antitrust laws. We do not engage in price fixing, market allocation, bid rigging, or any other anti-competitive practices.

6. EXPORT CONTROLS AND SANCTIONS

Opisense complies with all applicable EU and Norwegian export control regulations and international sanctions regimes. The Service may not be provided to any person, entity, or country subject to EU, US, or Norwegian sanctions. All personnel must comply with screening requirements and report any suspected sanctions violations immediately.

7. WORKPLACE CONDUCT

7.1 RESPECT AND INCLUSION

Opisense is committed to maintaining a workplace free from discrimination, harassment, bullying, and retaliation. All individuals are treated with dignity and respect, regardless of gender, gender identity, sexual orientation, ethnicity, nationality, religion, disability, age, or any other protected characteristic. This commitment extends to all interactions, including with customers, partners, and the public.

7.2 HEALTH AND SAFETY

Opisense provides a safe and healthy working environment in accordance with the Norwegian Working Environment Act (Arbeidsmiljøloven). All personnel are expected to contribute to a positive working environment and to report any health or safety concerns.

8. ENVIRONMENTAL RESPONSIBILITY

Opisense acknowledges its responsibility to minimise its environmental impact. As a cloud-native software company, our primary environmental footprint relates to cloud infrastructure energy consumption. Opisense selects infrastructure providers (Hetzner, EU) that have committed to renewable energy targets. We prioritise efficient computing practices, avoid unnecessary data retention, and seek to reduce the environmental cost of AI processing where feasible.

9. REPORTING AND WHISTLEBLOWING

9.1 REPORTING CHANNELS

Any person who becomes aware of a potential violation of this Code, applicable law, or Opisense's policies is encouraged to report it through the following channels:

- Direct report to the CEO
- Email to contact@opisense.com
- External whistleblowing channel (to be established when team size requires it under the Norwegian Whistleblowing Act)

9.2 PROTECTION AGAINST RETALIATION

Opisense prohibits retaliation against any person who reports a concern in good faith, whether the report is ultimately substantiated or not. This protection applies regardless of whether the report is made internally or to an external authority. Retaliation includes dismissal, demotion, harassment, exclusion, or any other detrimental treatment.

9.3 INVESTIGATION

All reports are investigated promptly, fairly, and confidentially. The CEO is responsible for ensuring that investigations are conducted impartially and that appropriate corrective action is taken where a violation is confirmed.

10. COMPLIANCE AND MONITORING

This Code of Conduct is reviewed annually and updated as required by changes in applicable law, regulatory guidance, or business operations. Compliance with this Code is monitored through periodic internal reviews and is included in the scope of external audits where applicable, including ISO 27001 alignment assessments. All personnel are required to confirm that they have read and understood this Code upon joining Opisense and annually thereafter.

11. RELATIONSHIP TO OTHER DOCUMENTS

This Code of Conduct establishes general ethical principles and governance commitments. Detailed requirements are set out in the following documents, which take precedence for matters within their specific scope:

Document Scope

- AI Policy: AI governance, EU AI Act compliance, responsible AI obligations
- Data Processing Agreement: GDPR compliance, data processing obligations, sub-processor management
- Privacy Notice: Personal data collection, use, retention, and rights
- Acceptable Use Policy: Platform use restrictions, prohibited conduct, enforcement
- Security Whitepaper: Technical security architecture, controls, and certifications
- Information Security Policy: ISMS policy (internal, referenced by ISO 27001 scope)

Code of Conduct

Last updated: 9 June 2026

12. CONTACT

Details	Opisense AS
Organisation number	936 578 195
General	contact@opisense.com
Privacy	dpo@opisense.com
Security	security@opisense.com
Ethics	contact@opisense.com
Website	https://opisense.com

This Code of Conduct is publicly available at opisense.com/legal and applies to all persons acting on behalf of Opisense AS.

DATA PROTECTION CULTURE

Opisense maintains a strong data protection culture with the following core commitments:

- Customer data is never used for AI model training without explicit, documented customer consent
- All employees receive annual mandatory data protection training
- Breach notification procedures comply with: 48-hour customer notification and 72-hour DPA notification
- EU AI Act compliance is embedded in all AI development activities

AI SAFEGUARDS & EU AI ACT COMPLIANCE

- Article 4 (AI Literacy): All personnel involved in AI development/deployment receive mandatory literacy training
- Article 5 (Prohibited Practices): Opisense prohibits AI systems that violate fundamental rights or enable illegal activities
- Article 52 (Transparency): All AI interactions with end-users include clear disclosure of AI involvement

BREACH NOTIFICATION PROTOCOL

Upon discovery of a personal data breach:

- Internal notification within 1 hour
- Customer notification within 48 hours
- Data Protection Authority notification within 72 hours
- Full incident report documentation

SUB-PROCESSOR & VENDOR MANAGEMENT

Sub-processor changes are managed with minimum 30 days advance written notice to Customers. All sub-processors execute Data Processing Agreements (DPAs) that comply with GDPR Article 28.

Code of Conduct

Last updated: 9 June 2026

INFRASTRUCTURE & SECURITY

- Primary data residency: Hetzner EU (Germany and Finland)
- Encryption: TLS 1.2+ minimum for all data in transit
- Post-termination: All customer data deleted within 60 days per DPA Section 11.3

ANNUAL CONFIRMATION

All Opisense personnel confirm compliance with this Code of Conduct annually. Breaches are subject to disciplinary action up to and including termination of employment.