AI Policy

Last updated: 9 June 2026

1. EXECUTIVE SUMMARY

Opisense AS is committed to the responsible, ethical, and transparent development and deployment of artificial intelligence (AI) systems. This policy articulates our commitment to compliance with the EU Regulation 2024/1143 on Artificial Intelligence (EU AI Act), the General Data Protection Regulation (GDPR), the Network and Information Security Directive 2022/2555 (NIS2), and internationally recognized AI governance standards.

Our AI systems are classified as limited-risk under the EU AI Act. We maintain comprehensive technical documentation, conduct Fundamental Rights Impact Assessments (FRIA), implement bias mitigation strategies, and ensure transparent communication about AI-generated content to users and customers.

2. REGULATORY FRAMEWORK

2.1 APPLICABLE REGULATIONS

This policy is aligned with the following regulatory frameworks:

- EU Regulation 2024/1143 (EU AI Act)
- General Data Protection Regulation (GDPR)
- Network and Information Security Directive 2022/2555 (NIS2)
- NIST AI Risk Management Framework
- ISO 42001:2024 (target Q2 2026)

3. AI SYSTEM INVENTORY AND CLASSIFICATION

3.1 OVERVIEW

Pursuant to EU AI Act Article 6, this section provides a comprehensive inventory of all AI systems deployed by Opisense.

3.2 AI SYSTEMS REGISTRY

The following table lists all AI systems in operation, their risk classification, and regulatory basis:

AI System	Description	Risk Level	Primary Data Types	EU AI Act Basis
Conversational Agents	LLM-based dialogue for customer interaction	Limited-Risk	Text prompts	Art. 6(1)(a)
Voice Agents	Voice synthesis for automated customer service	Limited-Risk	Audio data	Art. 6(1)(a)
Document Processing	Document extraction and classification	Limited-Risk	Document text	Art. 6(1)(a)
Meeting Analysis	Transcription and summarization	Limited-Risk	Audio recordings	Art. 6(1)(a)
Web-Browsing Agents	Autonomous web navigation and interaction on the user's behalf	Limited-Risk	Web page content, URLs	Art. 6(1)(a)
Code-Execution Agents	Execution of AI-generated code in isolated sandboxes	Limited-Risk	Code and task data	Art. 6(1)(a)

3.3 CLASSIFICATION RATIONALE

All Opisense AI systems are classified as Limited-Risk under EU AI Act Article 6(1)(a) based on transparent design, human oversight, and technical documentation.

4. PROHIBITED PRACTICES (EU AI ACT ART. 5)

4.1 COMMITMENT

Opisense does not develop, deploy, or commission any AI systems that fall within the prohibited categories of Article 5.

- No social credit systems
- No real-time biometric identification in public spaces
- No emotion recognition for law enforcement
- No subliminal manipulation
- No practices targeting vulnerable groups

5. LITERACY AND TRANSPARENCY (EU AI ACT ART. 4 & ART. 50(4))

5.1 USER-FACING DISCLOSURES

Opisense implements clear disclosures regarding AI system use in the platform.

- **In-Product Labels:** Each AI-powered feature displays a badge indicating AI-Generated or AI-Assisted.
- **Feature Documentation:** Help center explains which features use AI and what data each system processes.

5.2 MACHINE-READABLE MARKING (EU AI ACT ART. 50(4))

In addition to human-readable labels, Opisense implements machine-readable indicators:

- **API Response Headers:** All AI-generated content endpoints include metadata: X-Generated-By: AI, X-Processing-Via: [system-name].
- **JSON-LD Structured Data:** Web pages with AI-generated content include JSON-LD markup with @type AiGeneratedContent.
- **Metadata Tags in Documents:** Exported documents include metadata tags documenting AI generation, model, and timestamp.

6. TECHNICAL DOCUMENTATION (EU AI ACT ART. 11, ANNEX IV)

6.1 OVERVIEW

Opisense maintains technical documentation for each limited-risk AI system per Annex IV requirements.

6.2 DOCUMENTATION INCLUDES

- **System Description:** Intended use, target market, supported processes
- **Data Specifications:** Input types, sources, retention periods
- **Algorithm Details:** Model type, version, fine-tuning approach, performance metrics
- **Testing Results:** Test datasets, accuracy metrics, bias testing results
- **Risk Mitigation:** Controls addressing identified risks
- **Performance Monitoring:** KPIs tracked post-deployment

7. FUNDAMENTAL RIGHTS IMPACT ASSESSMENT (EU AI ACT ART. 27)

7.1 OVERVIEW

Pursuant to EU AI Act Article 27(1), Opisense has conducted a Fundamental Rights Impact Assessment (FRIA) for all AI systems.

7.2 FUNDAMENTAL RIGHTS POTENTIALLY AFFECTED

Analysis identifies the following fundamental rights:

- **Right to Data Protection:** AI systems process customer data; fairness and accuracy affect data subject rights
- **Right to Non-Discrimination:** Systems may inadvertently reflect biases; continuous monitoring is required
- **Right to Fair Trial:** AI outputs may inform business decisions; transparency mechanisms are essential
- **Right to Freedom of Expression:** Voice and document processing intersects with user-generated content
- **Right to Privacy:** Collection requires appropriate consent and safeguards

7.3 GROUPS POTENTIALLY IMPACTED

The following groups may be affected:

- Platform Customers
- End Users of Customers
- Vulnerable Populations (children, elderly, disabled individuals)
- Indirect Beneficiaries affected by AI-informed decisions

7.4 RISK MITIGATION MEASURES

Opisense implements controls to mitigate identified risks:

- **Data Protection:** Encryption, access controls, automated purging per GDPR Article 5(1)(e)
- **Bias Detection:** Quarterly fairness audits using industry metrics
- **Transparency:** In-product explanations and documentation of model limitations
- **Human Oversight:** High-consequence outputs flagged for human review
- **Contestation:** End users can request explanations and corrections
- **Sub-processor Governance:** Contractual control retained over sub-processor services

7.5 MONITORING AND REVIEW

Fundamental rights impacts are monitored through:

- **Incident Reporting:** Complaints logged and escalated
- **Quarterly Audits:** Fairness and accuracy metrics reviewed
- **Annual FRIA Review:** Full reassessment of impacts and mitigation
- **Customer Feedback:** Aggregated feedback analyzed for emerging rights issues
- **External Certification:** ISO 42001 and third-party bias audit pursuits

8. BIAS AND FAIRNESS ASSESSMENT

8.1 COMMITMENT

Opisense is committed to preventing unfair, discriminatory, or biased outputs.

8.2 BIAS TESTING FRAMEWORK

For each AI system, Opisense conducts:

- Pre-deployment bias audits
- Quarterly post-deployment fairness audits
- Red-teaming exercises
- Customer feedback loops

8.3 FAIRNESS METRICS

Fairness is assessed using industry-standard metrics including demographic parity, equalized odds, calibration, and individual fairness.

8.4 REMEDIATION

Where bias is detected, Opisense takes prompt action: model retraining, threshold adjustment, or feature removal.

9. EXPLAINABILITY AND TRANSPARENCY FRAMEWORK

All AI system outputs are accompanied by explanations of reasoning and data inputs used.

10. CONTENT LABELLING AND MACHINE-READABLE MARKING

See Section 5.2 for detailed requirements on machine-readable marking and metadata implementation.

11. INCIDENT REPORTING AND MANAGEMENT (EU AI ACT ART. 62)

11.1 OVERVIEW

Pursuant to EU AI Act Article 62, Opisense has established procedures for identifying, reporting, and investigating serious incidents.

11.2 DEFINITION OF REPORTABLE AI INCIDENT

A serious incident or malfunction means any occurrence with potential to cause:

- Injury or death to a person
- Substantial damage to property (>EUR 50,000)
- Significant impact on fundamental rights
- Platform unavailability >4 hours
- System behavior deviation from specifications
- Regulatory violation due to AI malfunction

11.3 INCIDENT REPORTING TIMELINE

Upon detection, logged in ISMS.

Preliminary investigation completed; mitigation initiated.

Assessment determines reportability.

If incident involves GDPR or AI Act breach with personal data, notification to Norwegian Data Protection Authority.

11.4 INCIDENT NOTIFICATION CONTENT

Notification to regulatory authority includes:

- **Incident Description:** What occurred, when detected, systems affected
- **Scope:** Number of data subjects impacted, data types, geographic scope
- **Root Cause:** Technical or operational failure
- **Immediate Mitigation:** Actions taken to stop and prevent recurrence
- **Affected Rights:** Which fundamental rights or GDPR articles were impacted
- **Contact:** Incident Response Officer and DPO contact details

11.5 INTERNAL ESCALATION PROCEDURE

Upon detection of serious incident:

- Step 1: Engineering team isolates affected systems
- Step 2: Security & Compliance teams notified; incident logged
- Step 3: DPO notified within 4 hours if personal data affected
- Step 4: Legal prepares regulatory notification within 48 hours
- Step 5: Executive briefing for Critical/High incidents
- Step 6: Customer notification prepared in parallel

11.6 POST-INCIDENT REVIEW PROCESS

Within 5 business days of closure:

- Root cause analysis (RCA) completed
- Corrective actions identified and prioritized
- Process improvements proposed
- Findings reviewed by Engineering, Security, Compliance
- Post-Incident Report filed within 15 days
- Lessons learned shared; training updated
- Follow-up testing scheduled to confirm corrections

12. DATA PROTECTION AND NON-TRAINING COMMITMENTS

12.1 DATA USE FOR TRAINING

Customer data is not used to train or fine-tune Opisense proprietary AI systems. Where sub-processors access customer data for third-party model inference (e.g., OpenAI, Anthropic), those sub-processors' terms apply; Opisense has obtained contractual undertakings that such data is not used for model training.

12.2 DATA RETENTION

AI inference logs are retained only for troubleshooting and quality assurance, then purged per GDPR Article 5(1)(e).

13. SUB-PROCESSOR AI SERVICES

Opisense engages the following sub-processors, all bound by DPA and non-training restrictions:

- OpenAI
- Anthropic
- ElevenLabs (voice synthesis)
- OpenRouter (LLM gateway; EU in-region routing)
- Browserbase (agent web browsing)
- Daytona (secure code execution)

14. GOVERNANCE AND ACCOUNTABILITY

AI governance overseen by:

- Chief Compliance Officer
- Data Protection Officer
- AI Ethics Lead
- Security Officer

15. CUSTOMER RESPONSIBILITIES

Customers must:

- Ensure lawful basis for processing personal data through AI
- Implement safeguards for sensitive data before upload
- Maintain consent records where required
- Notify data subjects of AI processing
- Handle incident reports in compliance with GDPR