RestaurangAI

restaurangai.se

EU AI Act
Technical Assessment

Comprehensive compliance analysis of RestaurangAI's AI systems under EU Regulation 2024/1689 (EU AI Act).

✓ **All systems: Limited Risk / Minimal Risk — No High-Risk AI**

Prepared for: RestaurangAI Tech Sweden & regulatory review

Date: March 4, 2026 | **Version:** 1.2

Classification: Confidential

Contact: info@restaurangai.se

Executive Summary

RestaurangAI is a Swedish AI-powered B2B SaaS platform providing intelligent automation for the restaurant industry. This document provides a technical assessment of all AI systems under EU AI Act (Regulation 2024/1689) compliance requirements.

> **Key Finding**
>
> All RestaurangAI AI systems are classified as **Limited Risk** or **Minimal Risk**. No high-risk AI systems are deployed.
>
> Primary obligation: Transparency requirements under **Article 50** — inform users they are interacting with AI.
>
> Full Article 50 compliance deadline: **August 2, 2026**

1. Company Overview

Attribute	Details
Company	RestaurangAI Tech Sweden
Website	www.restaurangai.se
Jurisdiction	Sweden (EU Member State)
Industry	Restaurant Technology / AI SaaS
Target Market	Swedish restaurants, cafés, and hospitality businesses
Supervisory Authority	Integritetsskyddsmyndigheten (IMY), Sweden

2. AI Systems Inventory

2.1 Voice AI Assistant ("AI-Hovmästaren Voice")

Attribute	Specification
Purpose	Automated phone booking and customer service
AI Model	Google Gemini 2.0 Flash (gemini-2.0-flash-exp)
Voice Provider	Twilio Media Streams + ElevenLabs (Swedish voice synthesis)
Telephony	Twilio Inc. (EU routing via Dublin, Ireland)
Language	Swedish (sv-SE)
Deployment	Real-time WebSocket streaming

Data Processing	Audio transcription (max 24h retention), intent detection, booking management

2.2 Conversational AI Chatbot ("AI-Hovmästaren Chat")

Attribute	Specification
Purpose	Customer inquiries, FAQ, booking, lead capture
AI Model	Google Gemini (via n8n AI Agent node)
Knowledge Base	Qdrant Vector Database (RAG architecture)
Channels	Facebook Messenger, Instagram, Web Widget, Custom Webhooks
Memory	PostgreSQL persistent chat history (12 months retention)
Orchestration	n8n workflow automation

2.3 AI Marketing Automation ("AI-Marknadsföraren")

Attribute	Specification
Purpose	Automated social media content generation and publishing
AI Model	Google Gemini (text generation + image prompts)
Channels	Facebook Pages, Instagram Business (via Meta Graph API)
Content Labeling	#SkapatMedAI on all AI-generated posts (Art. 50.4 compliance)
Human Oversight	Customer approval required before publishing

2.4 Analytics & Recommendation Engine ("AI-Restaurangchef")

Attribute	Specification
Purpose	Business intelligence and operational recommendations
AI Model	Google Gemini + rule-based statistical analysis
Data Sources	Internal KPI data, booking history, menu performance
Output	Recommendations only — no autonomous decisions

3. EU AI Act Risk Classification

3.1 Classification Framework

Risk Level	Description	Regulatory Approach
Unacceptable	AI posing clear threats to safety, rights	Prohibited
High Risk	AI in critical areas (health, employment, law enforcement)	Strict requirements
Limited Risk	AI interacting with humans	Transparency obligations (Art. 50)
Minimal Risk	All other AI systems	Voluntary codes of conduct

3.2 RestaurangAI System Classifications

AI System	Risk Category	Justification
Voice AI (AI-Hovmästaren Voice)	**Limited Risk**	AI interacting with persons via voice (Art. 50.1)
Chatbot (AI-Hovmästaren Chat)	**Limited Risk**	AI interacting with persons via text (Art. 50.1)
AI-Marknadsföraren	**Limited Risk**	AI-generated content on social media (Art. 50.4)
KPI Analytics / AI-Restaurangchef	**Minimal Risk**	Internal business analytics, no direct human interaction

3.3 High-Risk Exclusion Analysis

RestaurangAI systems do NOT fall under high-risk categories (Art. 6, Annex III) because they:

- Do not perform biometric identification
- Do not manage critical infrastructure
- Do not make employment decisions
- Do not assess creditworthiness
- Do not assist law enforcement or border control
- Do not process asylum or visa applications
- Do not perform profiling of natural persons (Art. 6.3)

> **Article 6 Assessment Result**
>
> Article 6(1) — Annex I Products: **NOT APPLICABLE**
>
> Article 6(2) — Annex III Categories: **NOT APPLICABLE**
>
> Profiling of natural persons: **NO PROFILING**
>
> **FINAL CLASSIFICATION: LIMITED RISK (Article 50 obligations apply)**

4. Technical Architecture

4.1 Infrastructure Overview

Component	Technology	Location
Server Hosting	Hetzner Cloud VPS (Docker Compose)	Helsinki, Finland (EU)
Reverse Proxy	Nginx + SSL/TLS (Let's Encrypt)	EU
Workflow Orchestration	n8n v2.8.1 (self-hosted)	EU (on-server)
Primary Database	PostgreSQL 16 with Row-Level Security	EU (on-server)
Vector Database	Qdrant (RAG knowledge base)	EU (on-server)
Cache / Queue	Redis	EU (on-server)

4.2 External AI Providers

Provider	Service	Data Sent	Data Retention
Google LLC	Gemini API (chatbot, voice, content)	Conversation text, prompts	Zero retention (EU data residency)
ElevenLabs Inc.	Voice synthesis (TTS)	Text to synthesize	Real-time only, no storage
Twilio Inc.	Telephony platform	Call metadata, audio stream	Metadata 12 months; audio real-time only
Meta Platforms Ireland	Messenger / Instagram API	Message content, page tokens	Per Meta DPA (EU entity)
Anthropic PBC	Claude API (internal analysis)	Internal prompts only	Zero retention

5. Transparency & Disclosure Compliance (Art. 50)

5.1 Implementation Status

Requirement	Status	Implementation
AI Disclosure (Voice) — Art. 50.1	✓ Implemented	Opening message identifies AI: "Hej! Du talar med [Restaurang]s AI-assistent."
AI Disclosure (Chat) — Art. 50.1	✓ Implemented	Welcome message identifies AI nature at conversation start
Human Escalation	✓ Implemented	Say "människa" (voice) or click button (chat) to reach human
AI-Generated Content Labeling — Art. 50.4	✓ Implemented	#SkapatMedAI on all AI-generated social media posts
Customer Approval Before Publishing	✓ Implemented	Portal approval step required before any post goes live

5.2 Disclosure Messages

Voice AI opening message:

> "Hej! Du talar med [Restaurangnamn]s AI-assistent. Hur kan jag hjälpa dig idag? Om du vill prata med en person, säg bara 'människa'."

Chatbot opening message:

> "Hej! Jag är en AI-assistent för [Restaurangnamn]. Ställ gärna frågor om menyn, öppettider eller boka bord. Vill du prata med en person? Skriv 'människa'."

6. Data Governance & GDPR Alignment

6.1 Personal Data Retention

Data Category	Retention	Legal Basis

Chat transcripts (AI-Hovmästaren)	12 months	Contract / Legitimate interest
Voice transcription	Max 24 hours	Contract performance (deleted automatically)
Voice call metadata	12 months	Billing / statistics
Contact details (active customers)	Contract + 36 months	Contract
Leads / inquiries	12 months from last contact	Consent (auto-deleted)
Invoices / accounting	7 years	Legal obligation (Bokföringslagen)
AI-generated content	Contract + 6 months	Contract

6.2 Security Measures

Measure	Implementation
Encryption at rest	AES-256 for credentials (PostgreSQL pgcrypto)
Encryption in transit	TLS 1.3 (HTTPS, WSS)
Access control	Row-Level Security (RLS) on all customer data tables
Audit logging	Immutable access logs, 12 months retention
Multi-tenancy isolation	restaurant_id enforced on all queries
Offsite backup	Daily encrypted backup to Google Drive (30-day retention)

6.3 Data Subject Rights

Right	Implementation
Right to Access (Art. 15)	SQL export via admin, delivered within 30 days
Right to Erasure (Art. 17)	CASCADE DELETE on restaurant / customer deletion
Right to Rectification (Art. 16)	Admin dashboard editing
Right to Portability (Art. 20)	JSON / CSV export available
Voice Data Deletion	Automatic within 24h; gdpr_deletion_log table maintained

7. Human Oversight

RestaurangAI implements a **Human-on-the-Loop (HOTL)** oversight model:

Component	Human Oversight Mechanism
Voice AI	Customer says "människa" → transferred to restaurant staff
Chatbot	"Prata med en person" option triggers handoff
AI-Marknadsföraren	All posts require customer approval in portal before publishing

| AI-Restaurangchef | Recommendations only — human decides on all actions |
| System Override | Restaurant owners can disable AI features at any time via portal |

8. Compliance Roadmap

Date	Milestone	Status
Feb 2, 2025	Prohibited AI practices in effect	✓ Compliant
Feb 2, 2025	AI Literacy requirements	✓ Compliant
Aug 2, 2026	Full Art. 50 transparency compliance	✓ Implemented
Aug 2, 2026	AI-generated content labeling (Art. 50.4)	✓ Implemented (#SkapatMedAI)
Ongoing	Art. 49(2) system registration when register opens	Pending (register not yet open)

9. Roles & Responsibilities

Role (EU AI Act)	Entity	Responsibilities
Provider	RestaurangAI Tech Sweden	When developing own AI features and workflows
Deployer	RestaurangAI Tech Sweden	When using third-party AI (Google Gemini, ElevenLabs, Anthropic)
Deployer	Restaurant customers	When using the RestaurangAI platform for their guests

10. Summary & Conclusions

Requirement	Status
Risk Classification (Art. 6)	✓ Completed — All Limited/Minimal Risk
Prohibited AI Check	✓ Compliant — No prohibited practices
AI Disclosure — Voice & Chat (Art. 50.1)	✓ Implemented
AI Content Labeling (Art. 50.4)	✓ Implemented (#SkapatMedAI)
Human Oversight / Escalation	✓ Implemented
Technical Documentation	✓ This document
Logging & Auditability	✓ Implemented (12 months)
GDPR Alignment	✓ Compliant
Art. 49(2) System Registration	Pending — EU register not yet operational

Key Findings

- **No High-Risk AI:** All systems classified as Limited Risk or Minimal Risk.

- **Art. 50 Compliant:** AI disclosure implemented in Voice, Chat, and content labeling (#SkapatMedAI).

- **GDPR Foundation:** Existing GDPR measures provide strong basis for AI Act compliance.

- **AI Stack:** Google Gemini (primary LLM), ElevenLabs (voice synthesis), Twilio (telephony), Meta (social channels), Anthropic (internal analysis only).

Contact

Role	Contact
Technical & Compliance	info@restaurangai.se
Website	www.restaurangai.se