AI Policy - Meetric Conversation Intelligence Platform

Meetric is committed to the responsible development and deployment of artificial intelligence. This AI Policy sets out our approach to transparency, accountability, and compliance in relation to our AI-powered conversation intelligence platform. It is designed to inform our customers, users, and stakeholders about how we develop, deploy, and govern AI systems, and to demonstrate our commitment to ethical AI practices in accordance with applicable regulatory frameworks, including the EU AI Act and the General Data Protection Regulation (GDPR). This Policy should be read in conjunction with our Data Processing Agreement and Privacy Policy.

Definitions

For the purposes of this policy, these terms are defined as follows:

AI-Generated Content: Any output automatically produced by our AI systems, including transcriptions, summaries, analytics, and insights.

Anonymisation: The irreversible process of transforming personal data in such a way that the data subject is no longer identifiable by any means reasonably likely to be used. Once properly anonymised, data falls outside the scope of GDPR.

Personal Data: Any information relating to an identified or identifiable person, including but not limited to names, contact details, voice recordings, and professional information captured in conversations.

~~**Pseudonymization:** The process of replacing identifying information with artificial identifiers ("tokens") that maintain analytical value while protecting individual privacy. Original identifying information is stored separately and securely.~~

Source Material: Original recordings, transcripts, or text data from which AI insights are derived. This serves as the verifiable basis for all AI-generated analysis.

Human Oversight: Direct human supervision and review of AI system outputs, including the ability to verify, override, or correct AI-generated insights.

Insights: Patterns, trends, or observations automatically identified by our AI systems, always presented with clear links to supporting evidence in source materials.

User: Any person authorized to access and use the platform's AI capabilities, including employees, administrators, and designated third parties where applicable.

1. System Classification and Scope

1.1 System Description

Meetric provides an AI-enhanced conversation intelligence platform that processes audio & video recordings and textual data like email and chat from customer and internal business conversations. The AI functionalities we employ include but are not limited to:

- Automated speech-to-text transcription
- Speaker identification and diarization
- Natural language processing for conversation analysis
- Automated summarization
- Conversation pattern recognition
- AI analysis of process fulfilment in conversations

Our AI capabilities combine proprietary systems that we host and maintain with select third-party Large Language Models (LLMs). The balance between in-house and third-party technologies varies by application, and we continuously evaluate and adapt this mix based on evolving needs and available alternatives.

1.2 Third-Party LLM Providers

We currently use Google Gemini (provided by Google Cloud EMEA Limited, Ireland) as our primary third-party Large Language Model provider. All third-party LLM providers are established and operating within the EU/EEA, engaged as sub-processors under formal Data Processing Agreements, subject to contractual prohibitions on using customer data for training or retention, and listed as sub-processors in our Data Processing Agreement or in an equivalent sub-processor list agreed with each customer. We continuously evaluate LLM providers to ensure optimal performance, security, and compliance with data protection requirements.

1.3~~1.2~~ Risk Classification

Our platform's risk classification varies based on specific use contexts and implementation:

The risk classifications set out below represent Meetric's preliminary assessment based on typical use cases. Customers are responsible for conducting their own risk assessment based on their specific use context, implementation, and the requirements of the EU AI Act. The final risk classification for any particular deployment depends on factors including the specific use case, the role of AI outputs in decision-making processes, and the categories of individuals affected.

Limited Risk Use Cases

These are our standard applications where the AI system serves as a supportive tool without direct impact on decisions:

- Meeting transcription to create searchable text records of conversations
- Basic conversation analytics identifying topics and themes
- Process adherence insights with clear references to source material
- Team communication pattern analysis for improvement opportunities

Elevated Risk Contexts

While our platform remains a supportive analytical tool, additional safeguards are implemented when used in:

- Employee development contexts where insights may inform training needs
- Quality assurance scenarios where conversation patterns are analyzed
- Process compliance monitoring where adherence to procedures is tracked
- Sales or customer service settings where interaction patterns are studied

Risk Management Approach

Our platform maintains strict operational boundaries:

- Functions solely as an analytical tool without autonomous decision-making
- All insights link directly to source material for verification
- Serves in a supportive capacity to human decision-makers
- Provides transparency in how conclusions are reached
- Maintaining clear "human-in-the-loop" design principles
- Ensuring traceability between insights and source data
- Implementing mandatory human review checkpoints

To ensure responsible deployment:

- Regular risk assessments for all use cases
- Comprehensive safeguards applied proactively

- Compliance with high-risk system requirements where applicable
- Continuous monitoring and adjustment of safety measures

2. Technical Specifications and Safeguards

2.1 Data Processing Framework

Our system processes personal data in the following manner:

EU/EEA-Based Processing

- All personal~~audio~~ data, including data ~~is~~ processed by third-party Large Language Models (LLMs), is handled exclusively within EU/EEA~~-based~~ infrastructure:~~:~~
  - ~~Data sent to~~ third-party LLM providers are established~~LLMs undergoes a comprehensive pseudonymization process that includes:~~
    - ~~Replacement of all personally identifiable information (PII) with unique tokens~~
    - ~~Automated detection~~ and operate within the EU/EEA.~~masking of:~~
    - All processing occurs on servers located within EU/EEA regions.
      - ~~No personal~~~~Names, email addresses, and phone numbers~~
      - ~~Employee IDs and user identifiers~~
      - ~~Customer account numbers and reference codes~~
      - ~~Physical addresses and location~~ data is transferred outside
      - ~~Financial and transaction details~~
      - ~~Context-aware identification and replacement of indirect identifiers~~
    - ~~Verification checks to ensure no PII patterns remain in the processed text~~
    - ~~Maintenance of a secure mapping table for token restoration, stored separately from~~ the EU/EEA.~~pseudonymized data~~
    - All LLM providers are engaged as sub-processors under applicable data processing agreements with appropriate contractual safeguards.

Contractual Safeguards with LLM Providers

- ~~Regular audits of pseudonymization effectiveness~~

~~The pseudonymized data maintains analytical utility while ensuring no individual can be identified from the data sent to third-party LLMs alone, without access to the separately stored mapping information.~~

Third-party LLM providers are contractually prohibited from:

- Using processed data to train or improve their AI models
- Storing our data beyond the immediate processing need
- Using our data for any purpose other than delivering the requested analysis
- Transferring data outside the EU/EEA

Additional Data Protection Measures

- End-to-end encryption for all data in transit and at rest
- Processing occurs in isolated environments with strict access controls.
- Data minimi~~s~~zation principles are applied throughout.
- Retention periods are clearly defined and automatically enforced (real-time or near-real-time processing with no retention beyond the processing session).~~.~~
- All insights and analysis are directly linked to source material through precise timestamps.
- The system maintains a verifiable chain of evidence by always referencing original recordings and transcriptions.
- No autonomous decisions are made by the platform; all insights are presented as suggestions with clear links to supporting evidence.

Users retain full control over decision-making, with the platform serving purely as an analytical tool.

Meetric acts as a Data Processor with respect to customer data. We process personal data only on the documented instructions of our customers, as set out in the applicable Data Processing Agreement and related contractual documentation, and we ensure that any sub-processors are bound by equivalent obligations.

2.2 Risk Management System

We maintain a comprehensive risk management system that includes:

- Regular algorithmic impact assessments

- Continuous monitoring of system outputs
- Bias detection and mitigation procedures
- Regular security vulnerability assessments
- Incident response protocols

2.3 Data Governance

- Personal data handling includes: End-to-end encryption for all data in transit and at rest.
- ~~End-to-end encryption for all data in transit and at rest~~
- ~~Automated anonymization where applicable~~
- Role-based access control
- Data minimization by design
- Clear data deletion procedures
- Anonymisation in accordance with our Data Processing Agreement and our customers' documented instructions

2.4 Anonymisation and Use of Anonymised Data

Anonymisation Process

Where appropriate and in accordance with our Data Processing Agreement and the documented instructions of our customers, Meetric may anonymise conversation data using industry-standard techniques that ensure:

- The data subject is no longer identifiable by any means reasonably likely to be used
- The anonymisation is irreversible and cannot be re-identified
- The process does not reveal personal data, business secrets, or confidential information

Use of Anonymised Data

Once data has been effectively anonymised and falls outside the scope of GDPR, Meetric may use such data for analysing and monitoring platform performance and effectiveness, improving and developing AI models and algorithms, training and testing AI systems, conducting statistical analysis and research, and product development and enhancement.

Safeguards

To ensure ongoing protection of individuals and organisations, Meetric maintains documentation of anonymisation techniques and processes, applies technical and organisational measures to prevent re-identification of anonymised data, conducts regular audits to verify the effectiveness of anonymisation, and maintains a clear distinction between anonymised data (outside GDPR scope) and pseudonymised data (still personal data under GDPR).

3. Transparency and Oversight

3.1 Documentation Requirements

We maintain detailed documentation of:

- System architecture and components
- Training data sources and validation procedures
- Risk assessment methodologies
- Testing and validation results
- Incident reports and resolution measures
- Change management logs

3.2 Human Oversight

Our human oversight framework ensures:

- Clear allocation of oversight responsibilities
- Regular review of system outputs
- Authority to override system decisions
- Continuous training for oversight personnel
- Clear escalation procedures

3.3 User Information

We provide users with:

- Clear identification of AI-generated content
- Explanation of system capabilities and limitations

- Information about human oversight options
- Guidelines for responsible system use
- Regular updates about system changes

4. Quality Management

4.1 Quality Measures

Our quality management system includes:

- Regular accuracy assessments
- Bias monitoring and mitigation
- Performance benchmarking
- Regular system audits
- Continuous improvement protocols

4.2 Monitoring and Reporting

We implement:

- Automated system monitoring
- Regular compliance assessments
- Incident tracking and reporting
- Performance metrics tracking
- User feedback collection and analysis

5. Compliance Commitment

5.1 Regulatory Updates

Our regulatory approach includes:

~~We commit to:~~

- Regular review of regulatory requirements
- Proactive compliance updates

- Engagement with regulatory bodies
- Industry standard alignment
- Transparent communication about changes

We have designed our systems to support~~And maintain comprehensive~~ compliance with:

- EU AI Act requirements ~~as detailed in this policy~~
- GDPR requirements, including provisions for AI-related processing of personal data, in our capacity as Data Processor acting on our customers' documented instructions pursuant to the applicable Data Processing Agreement
- ~~GDPR requirements as detailed in our DPA~~
- Emerging regulatory frameworks

For detailed GDPR compliance measures~~,~~ ~~and~~ data protection protocols, sub-processor information, and security measures, customers should~~please~~ refer to the~~our~~ Data Pro~~c~~tess~~c~~ti~~o~~ng Agreement in place between Meetric and the relevant customer, including any schedules or sub-processor listings agreed from time to time.

5.2 User Support

We provide:

- Dedicated compliance support
- Regular training materials
- Clear usage guidelines
- Prompt incident response
- Regular compliance updates

6. Compliance Framework~~Declaration of Conformity~~

Meetric has designed and implemented this system to support compliance with applicable AI regulations. In this regard:

~~We declare that:~~

- This system has been designed~~assessed for compliance~~ with ~~the~~ EU AI Act requirements in mind.

- Appropriate risk management measures are in place.
- Regular monitoring and updates are performed.
- Documentation is maintained and available for audit.
- Human oversight is implemented as required.

Customers remain responsible for assessing the risk classification applicable to their specific use of the platform and for ensuring that their deployment complies with the EU AI Act and other applicable regulations. Meetric will provide reasonable assistance to customers in conducting such assessments upon request.

Last Updated: 11 February 2026~~2025-02-19~~