LAB University of Applied Sciences

Moody APP
AI ACT Research

Mario Sanjuan, Raven, Airiss & Katrina

21-1-2026

Contents

1 Introduction

The Moody app is conceived as a personal AI assistant that allows users to send text messages or audio recordings about their daily experiences. The system analyzes these entries, infers patterns in thoughts and emotions, and responds with questions and reflections to help the user understand themselves and improve their wellbeing. This functionality places Moody at the intersection of artificial intelligence, mental health support, and sensitive personal data processing.

The European Union has adopted the EU Artificial Intelligence Act (AI Act), a risk-based regulatory framework for AI systems, and continues to enforce the General Data Protection Regulation (GDPR) for personal data protection. Because Moody processes intimate voice and text data and performs emotional and behavioral inferences, it is heavily impacted by both instruments. This document analyzes how the AI Act and GDPR apply to Moody and proposes a compliance and design strategy that enables ethical and lawful deployment.

2 App Concept and Technical Overview

Concept Overview Moody's core concept is an AI-powered *mood companion* focused on personal self-reflection rather than clinical therapy or workplace performance management.

User Journey

1. The user records an audio message or writes a text entry about their day.
2. The application transcribes audio to text, processes the content, and infers aspects such as mood, stressors, recurrent themes, and behavioral patterns.
3. The AI agent asks follow-up questions, offers supportive reflections, and proposes small actions aimed at improving self-understanding and self-care.

Technical Architecture

- Front-end mobile applications handling audio recording, playback, and chat-like interactions.
- Backend services responsible for automatic speech recognition (ASR), natural language processing (NLP), and emotional inference based on text and voice features.
- A personalization layer that incrementally builds a user-specific profile based on historical entries and interaction patterns.
- Data storage and analytics components that maintain voice recordings, text transcripts, derived features, and user configuration settings.

AI System Qualification This architecture qualifies Moody as an *AI system* under the AI Act, as it relies on machine-learning models to generate outputs that may influence users' behavior and decision-making processes.

3 Legal Framework: EU AI Act and GDPR

3.1 EU AI Act Overview

The AI Act introduces a risk-based regulatory model, distinguishing between unacceptable risk (prohibited), high-risk (heavily regulated), limited risk (transparency duties), and minimal risk (largely unregulated). Unacceptable practices include social scoring, certain types of manipulative systems, and specific uses of emotion recognition in workplaces and education.

High-risk systems are permitted but must comply with strict obligations covering risk management, data governance, transparency, human oversight, robustness, documentation and, in many cases, conformity assessments and registration with authorities.

3.2 GDPR Overview

GDPR governs the processing of personal data in the EU and applies fully to AI systems that store, analyze, or profile individuals. Voice recordings, transcripts, behavioral profiles, and inferred emotional states are all considered personal data. If entries reveal information about health, mental state, sexuality, religion, or political opinions, they constitute special category data, which is subject to additional protection and typically requires explicit consent.

GDPR imposes obligations on lawful basis, transparency, data minimization, purpose limitation, security, and the enforcement of data subject rights such as access, deletion, and portability. The regulation also requires a Data Protection Impact Assessment (DPIA) when large-scale processing of sensitive data or systematic profiling may significantly affect individuals.

4 Risk Classification of Moody Under the AI Act

4.1 Emotion Recognition and Biometric Processing

Moody analyzes voice recordings and text to infer emotional or mental states. Emotion recognition based on biometric data, such as voice, is explicitly addressed in the AI Act and corresponding guidance. Systems that infer emotions or mental states from biometric signals are considered emotion recognition systems and generally fall under the high-risk category when used in specified contexts or when they significantly affect individuals.

Key Characteristics Key characteristics of Moody include:

- The use of voice and linguistic patterns as biometric indicators of mood or mental state.
- Persistent profiling over time to build a nuanced and evolving picture of the user's inner life.
- Tailored feedback mechanisms that may influence users' emotions, perceptions, and decisions.

These characteristics strongly indicate that Moody should be treated as a *high-risk AI system*, even if it is marketed as a wellness-oriented application rather than a clinical or workplace tool.

4.2 Prohibited Use Cases to Avoid

The AI Act explicitly prohibits certain uses of emotion recognition systems, particularly in workplace and educational contexts, except under narrowly defined safety or health-related exceptions. Consequently, Moody must not be deployed, configured, or marketed as:

- An employee monitoring tool or performance evaluation system.
- A student monitoring solution for assessing classroom behavior or emotional engagement.
- A social scoring system that rates users' perceived *value* or *trustworthiness* and shares such assessments with third parties.

Explicitly excluding these use cases within product design decisions, contractual agreements, and marketing materials is essential to ensure compliance and to avoid classification under prohibited AI practices.

5 Compliance Obligations for Moody as a High-Risk AI System

5.1 Risk Management System

The AI Act requires providers of high-risk AI systems to establish a continuous and documented risk management framework. For Moody, this entails:

- Identifying risks such as erroneous emotional assessments, psychological harm, over-reliance on AI instead of professional support, privacy breaches, and bias against vulnerable groups.
- Evaluating the likelihood and potential impact of each identified risk across the entire system lifecycle.
- Implementing mitigation measures, including content filters, crisis escalation protocols, conservative default behaviors, and robust security controls.
- Monitoring system performance and reported harms post-deployment, and updating mitigation measures accordingly.

5.2 Data Governance and Quality

Training, validation, and operational datasets must comply with the AI Act's data governance requirements and be appropriate, representative, and as free from errors as practicable. For Moody:

- Data minimization principles should restrict collection to data strictly necessary for diary analysis and coaching, avoiding the capture of unrelated biometric or contextual information.
- Datasets used to train emotion recognition and language models should represent diverse genders, ages, cultures, and accents in order to reduce systemic bias.
- Data lineage, cleaning processes, and quality assurance procedures should be thoroughly documented, including methodologies for labeling or annotating emotional states.

5.3 Technical Documentation and Record-Keeping

Providers of high-risk AI systems must maintain comprehensive technical documentation describing the system's purpose, design, development, and risk controls. For Moody, this documentation should include:

- System architecture diagrams and detailed module descriptions.
- The algorithmic approach used for emotion inference and personalization.
- Summaries of training and testing datasets, including data sources and known limitations.

- Evaluation results addressing accuracy, robustness, and fairness.
- Descriptions of content safety filters, crisis-handling mechanisms, and user-control features.
- Logs documenting incidents, system updates, and risk management decisions.

5.4 Transparency, Information, and Human Oversight

The AI Act mandates clear transparency and user information obligations for high-risk AI systems. For Moody, this implies:

- Informing users that they are interacting with an AI-based system rather than a human whenever they engage with the assistant.
- Explaining that the system analyzes diary entries and infers emotional states to personalize responses, and that such inferences may be inaccurate or biased.
- Providing clear warnings that the application is not a medical or therapeutic service, and advising users to seek professional help for serious mental health concerns.
- Ensuring that the user interface enables meaningful oversight, including options to view and adjust personal settings, pause analysis, and review inferred behavioral or emotional patterns.

Human oversight in Moody is primarily exercised by the user themselves, supported by design constraints and safety mechanisms that prevent the system from making critical or irreversible decisions about the user.

5.5 Conformity Assessment and Registration

Prior to placing a high-risk AI system on the European Union market, providers must conduct or undergo a conformity assessment and register the system in the EU database of high-risk AI systems. For Moody, this will likely require:

- Internal compliance assessments against AI Act requirements set out in Articles 9–15, including risk management, data governance, documentation, transparency, human oversight, accuracy, and robustness.
- Preparation of the technical documentation and availability of supporting evidence for competent supervisory authorities.
- Registration of the system with the relevant authority, likely involving coordination with the Spanish Data Protection Authority (AEPD) for data protection and processing aspects.

6 GDPR Duties for Moody

6.1 Lawful Basis and Explicit Consent

Because Moody processes voice recordings and analyzes personal narratives that may reveal information related to health, mental state, sexuality, or personal beliefs, it handles *special category personal data*. The GDPR generally prohibits the processing of such data unless:

- The user provides explicit consent for clearly specified purposes, or
- Specific exemptions apply (e.g., medical or public health purposes), which is not the case for a commercial wellness application.

Moody must therefore rely on explicit and granular consent, obtained through clear and user-friendly consent flows that distinctly separate:

- Consent to record and store audio and text entries.
- Consent to analyze and profile emotional and behavioral patterns.
- Optional consent to use anonymized or aggregated data for model improvement or research purposes.

Consent must be freely given, informed, specific, and revocable at any time without detriment to the user.

6.2 Data Minimization, Purpose Limitation, and Security

The GDPR requires that personal data collection be limited to what is necessary for defined purposes, that data not be repurposed in incompatible ways, and that appropriate technical and organizational security measures be implemented. For Moody, this entails:

- Limiting data collection to diary content, essential metadata, and user configuration settings, while avoiding unnecessary third-party or contextual data.
- Using diary entries exclusively for personal coaching and, where explicit consent has been provided, for narrowly scoped research or model improvement, and explicitly prohibiting secondary uses such as targeted advertising, credit scoring, or employee monitoring.
- Implementing strong security safeguards, including encryption in transit and at rest, strict access controls, intrusion detection systems, and regular security assessments and testing.

6.3 Data Subject Rights and DPIA

Moody must enable the full exercise of GDPR data subject rights, including the rights of access, rectification, erasure, restriction of processing, data portability, and objection. In practical terms, this requires:

- In-application tools allowing users to access and download their data, including voice recordings, text transcripts, and inferred user profiles.
- Mechanisms to delete individual diary entries as well as entire user accounts, including the deletion of derived profiles where technically feasible.
- Options to pause data processing, disable personalization features, or opt out of secondary data uses.
- The provision of structured, commonly used, and machine-readable export formats to support data portability to other services.

Given the scale, sensitivity, and systematic profiling of personal data involved, Moody must conduct a *Data Protection Impact Assessment (DPIA)* prior to deployment. The DPIA should document data flows, assess risks to data subjects' rights and freedoms, and describe mitigation measures. Where high residual risks remain, prior consultation with the Spanish Data Protection Authority (AEPD) may be required.

7 Ethical Challenges

Beyond formal legal compliance, Moody raises several ethical concerns that must be addressed through careful system design and governance:

- **Psychological harm and over-reliance:** Users may come to treat the application as a substitute for professional therapy or crisis support. Inaccurate, incomplete, or biased feedback may unintentionally exacerbate emotional distress or delay access to appropriate help.
- **Manipulation and nudging:** Highly personalized insights and recommendations can influence user behavior. Depending on design and incentive structures, such nudging may be beneficial or may cross into manipulative or exploitative practices.
- **Bias and fairness:** Emotion and sentiment analysis models may perform unevenly across cultures, languages, accents, genders, and neurodiverse users, potentially leading to systematic misinterpretation or unequal quality of support.
- **Dignity and autonomy:** Continuous emotional monitoring and profiling may feel intrusive and can undermine users' sense of privacy, dignity, and autonomy if not accompanied by clear controls, transparency, and meaningful user choice.

Addressing these ethical challenges requires deliberate design decisions, ongoing evaluation, and governance measures that go beyond minimum regulatory compliance.

8 Design and Governance Solutions

8.1 Narrow and Explicit Scope

A foundational design and governance measure is to define and enforce a strict operational scope for Moody:

- Clearly positioning the application as a personal self-reflection and wellbeing tool intended for adult consumers.
- Explicitly prohibiting use in employment, education, law enforcement, credit, or insurance contexts through contractual terms and technical safeguards.
- Avoiding the implementation of social scoring, ranking, or reputational metrics that could be repurposed or misused by third parties.

This scoped approach limits Moody's exposure to the most sensitive and prohibited application areas under the AI Act.

8.2 Privacy- and Safety-by-Design

Moody should embed privacy and safety protections directly into its core product architecture:

- Implementing local or on-device preprocessing where feasible, such as temporary audio recording prior to secure upload.
- Applying strong encryption mechanisms and strict access controls, with comprehensive logging of all internal data access.
- Deploying content filters and protective response mechanisms for self-harm or crisis-related language, directing users to emergency services or helpline resources rather than providing substantive guidance.
- Including clear and prominent warnings indicating that the application is not a medical professional or therapist and that automated outputs may be inaccurate.

These measures reduce both the likelihood and potential impact of harm, while supporting GDPR privacy-by-design principles and the AI Act's risk management obligations.

8.3 Transparency, Explainability, and User Control

To foster user trust and meet transparency requirements, Moody should:

- Clearly label the assistant as an AI-based system and visibly mark AI-generated responses within the user interface.
- Explain, using accessible and non-technical language, what forms of analysis are performed (e.g., detection of emotional tone or recurring themes) and explicitly state what the system does not do (e.g., clinical diagnosis).
- Provide users with access to their inferred profiles and allow correction or deletion where outputs are perceived as inaccurate or harmful.
- Offer granular configuration options enabling users to disable specific analyses, such as emotion inference, while continuing to use the diary as a simple self-reflection tool.

These features provide users with meaningful oversight and control over how the system interprets and processes their data.

8.4 Robust Risk and Bias Management

Moody's governance framework should incorporate:

- Regular evaluation of model performance and error patterns, with specific attention to impacts across demographic subgroups.
- Bias testing across languages, accents, genders, age groups, and cultural contexts, with retraining or recalibration where significant disparities are identified.
- User feedback and reporting mechanisms for harmful, misleading, or inappropriate responses, with integration into ongoing risk assessment and model improvement processes.
- Periodic review of ethical guidelines by an internal or external advisory body, particularly when introducing new features or expanding system capabilities.

This continuous monitoring and governance approach aligns with the AI Act's post-market surveillance obligations for high-risk AI systems.

9 Implementation Roadmap

A practical roadmap for ensuring Moody's regulatory compliance and ethical design may include the following phases:

9.1 Initial Legal and Ethical Assessment

- Confirm the classification of Moody as a high-risk AI system and identify all applicable obligations under the AI Act.
- Map GDPR responsibilities, including the identification of a lawful basis for processing and the requirement to conduct a Data Protection Impact Assessment (DPIA).

9.2 Architecture and Policy Design

- Design system architecture and data flows in accordance with data minimization, purpose limitation, and security principles.
- Draft and review privacy policies, terms of service, consent language, and procedures for exercising user rights.

9.3 Risk Management and Documentation

- Establish and maintain a risk register and mitigation plan in line with AI Act Article 9 requirements.
- Prepare the technical documentation and complete DPIA records to support regulatory oversight and accountability.

9.4 Development and Testing

- Implement consent mechanisms, safety filters, encryption measures, and user control features within the product.
- Conduct functional testing, robustness evaluations, and fairness assessments across relevant user groups.

9.5 Conformity Assessment and Registration

- Perform an internal conformity assessment against applicable AI Act requirements.
- Register Moody as a high-risk AI system with the appropriate European Union authorities prior to market placement.

9.6 Launch and Continuous Monitoring

- Deploy post-launch monitoring mechanisms for incidents, performance issues, and user complaints.
- Periodically re-evaluate identified risks, update technical and legal documentation, and revise models and governance policies as necessary.

10 Conclusion

Moody's core idea—to analyze daily voice and text diaries and provide personalized, reflective support—falls within a highly sensitive regulatory space because it involves emotional inference and intensive profiling of intimate personal data. Under the EU AI Act, the system should be treated as a high-risk AI system, though it is not inherently prohibited if confined to consumer self-reflection use and carefully designed. Under GDPR, processing of voice-based diaries and inferred mental states requires explicit consent, strict data protection, and full support for user rights.

The "problem" is therefore not that Moody is impossible, but that it must be built with rigorous legal, technical, and ethical safeguards. By defining a narrow scope, avoiding prohibited use cases, implementing privacy- and safety-by-design, ensuring strong transparency and user control, and establishing robust risk and bias management, Moody can operate in a way that is both compliant with EU law and aligned with the wellbeing and autonomy of its users