

AI Act - Chatbot

...

A chatbot that answers questions
on the applicability of the EU AI Act and related regulation

AI Act

The AI Act, officially the European Union's Artificial Intelligence Act, is a comprehensive regulation designed to govern the development and use of artificial intelligence within the EU. It aims to ensure AI systems are safe, respect fundamental rights, and foster a harmonized single EU market for AI.

Chatbots

What are chatbots?

Chatbots are computer programs designed to simulate human conversation, either through text or voice interactions.

Are they helpful?

- Helpful as assistants.
- Used by businesses in many different contexts.
- They can serve many customers at the same time.
- 24/7 availability.
- Legal context: Help someone as their legal assistant.

Datasets

We took our dataset from „EUR-Lex” - Official access to European Union law

Link: <https://eur-lex.europa.eu/homepage.html?lang=en>

Our main focus was on the following legal acts:

- AI Act
- GDPR on data protection
- Data Act
- Data Governance Act

Chunking

- We split our texts into smaller pieces
- Better understanding of the data
- Higher efficiency in searching and retrieving info
- Avoiding memory overload

Embedding



Computers understand numbers, not human language, therefore we need to transform our text into numbers (=vectors). This process is called “**embedding**”.

Embedding is essential for:

- Semantic Search: Finding documents based on meaning rather than exact keyword matches.
- Reranking: Reordering search results to highlight the most relevant documents.

Model used: **multi-qa-mpnet-base-dot-v1** (768 dimensions)

Model



- Model used : gemma-2-2b-it by Google
- 2.61 billion parameters
- A heavier model might require access to external resources.

RAG

- RAG (Retrieval-Augmented Generation) is an AI framework that combines traditional approaches to information retrieval (ex. databases) with Large Language Models (LLM)
- RAGs aim to mitigate the issue with LLMs tending to hallucinate fabricated information by supplementing the model's input with relevant external context

Question: “What profiling means?”

Answer: “Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

Document: GDPR Act

Question: “What is high-risk AI?”

Answer: “High-risk AI systems are those that are designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.”

Document: Act: AI. Article 16. Obligations of providers of high-risk AI systems

Question: “What is an AI system?”

Answer: “An AI system is a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”

Document: Act: AI. Article 3. Definitions

Future Work

- Increase the amount of relevant data.
- Change to a “heavier” model to improve performance.
- Experiment with different types of embeddings (**BERT**, ELMo, etc.)

Thank you for your attention!

Made by:

-Paschalis Agapitos

-Piotr Aleksandrowicz

-Lakin Breeden

-Martyna Czwojdzńska

-Tomek Detlaf

-Mia Dymek

-Désirée Klingler

-Milada Matoušková

-Georgia Pantazi

-Agata Wyszowska

Project adviser: Jan Mizerka