



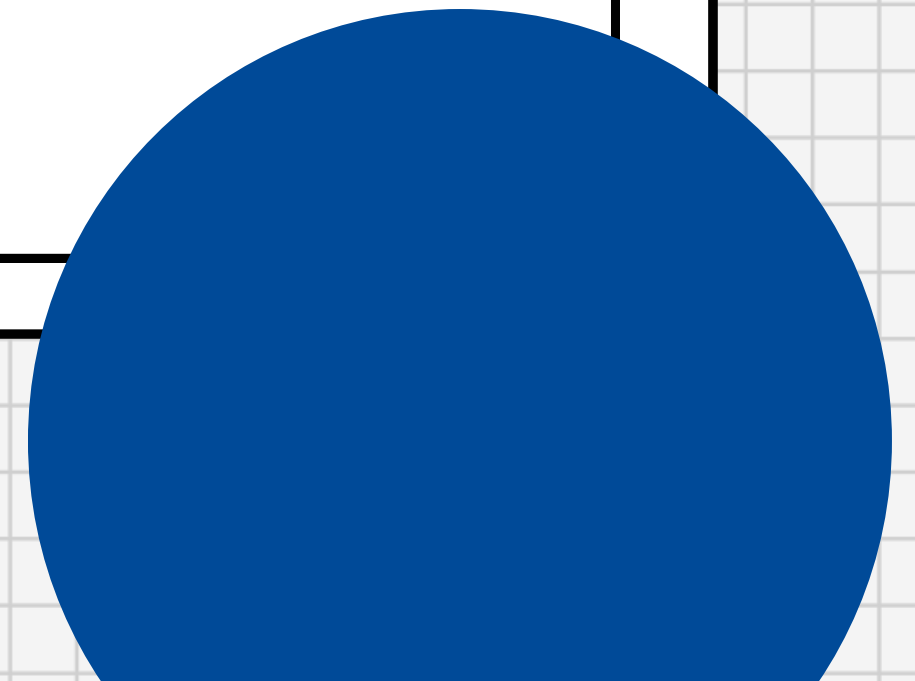
Break Through Tech AI Studio

12/06/2024

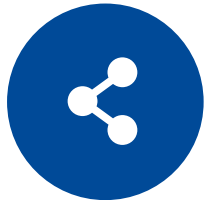


# DXC Technology 1B Presentation

Maya Swan, Nandini Shah, Gianelli Lagos, Pa Yang



# AGENDA:



+ Introduction & Problem Definition

+ Project Objectives & Research Approach

+ Data & Methodology

+ Evaluation & Insights

+ Conclusion & Discussion

# Meet the Team



Nandini Shah

University of  
Maryland

Computer  
Science



Gianelli Lagos

Stevens Institute  
of Technology

Computer  
Science



Pa Yang

Metropolitan State  
University

Data Science



Maya Swan

North Carolina A&T  
State University

Computer  
Science



Introduction



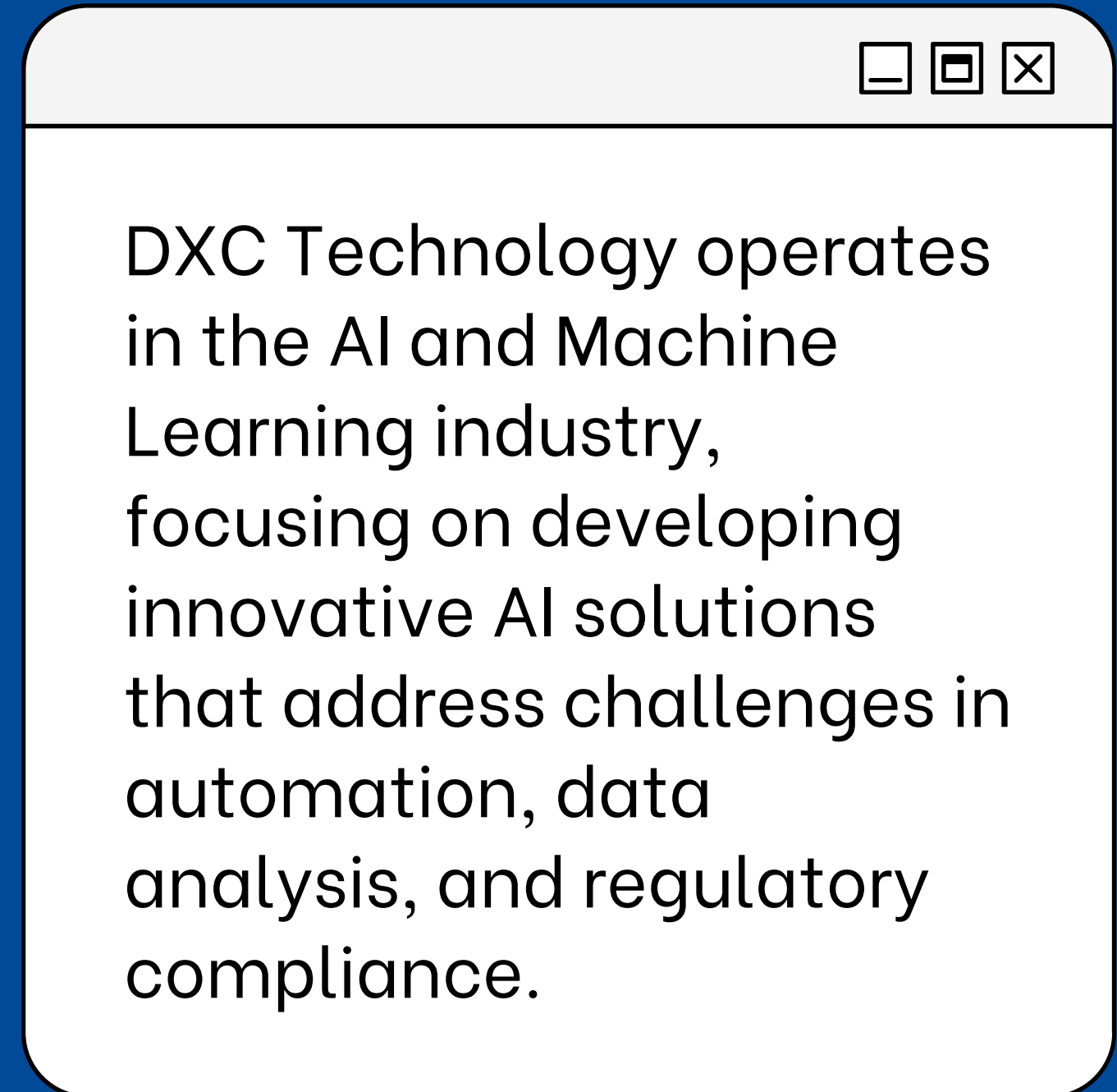
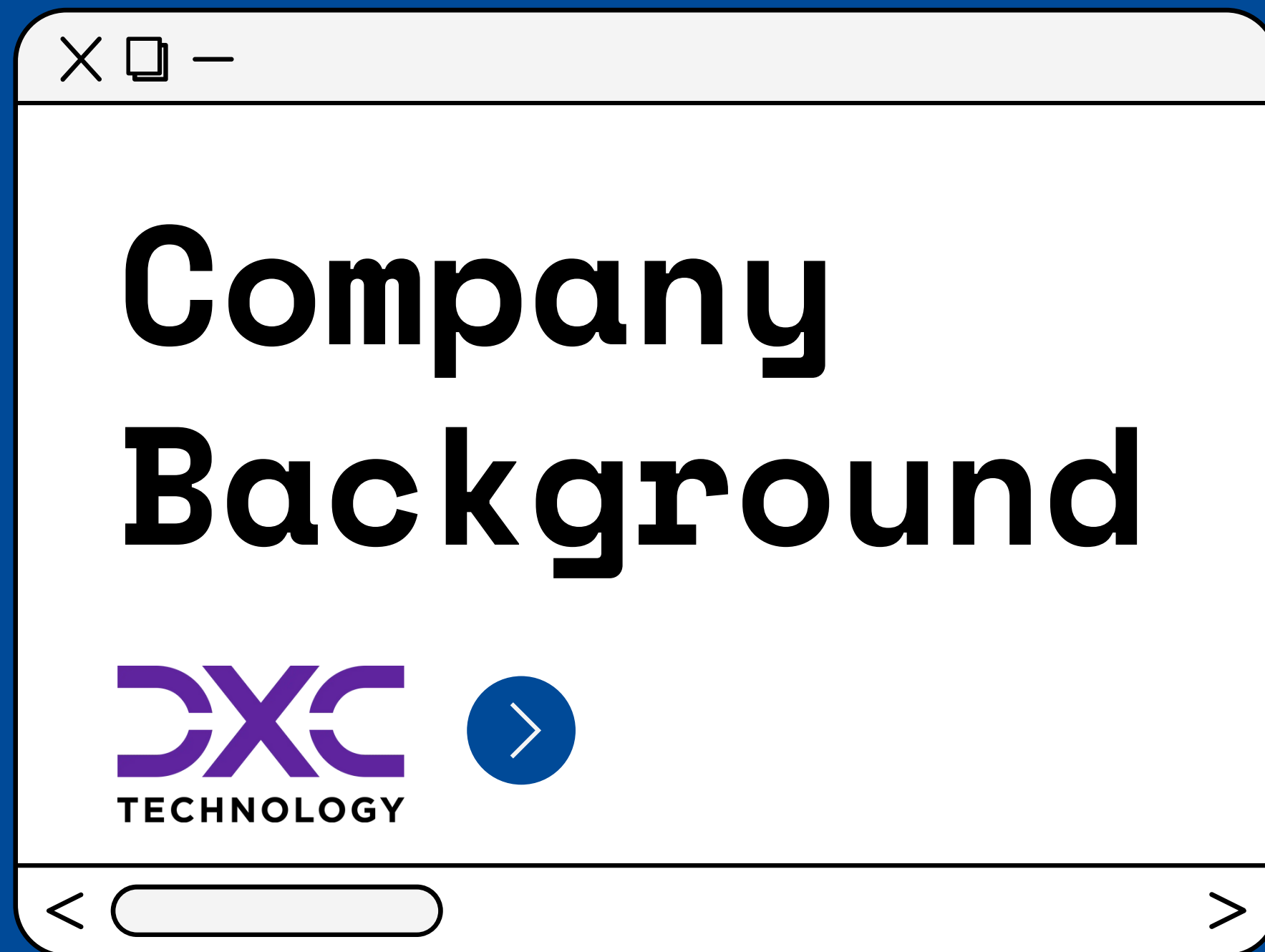
Research



Model



Conclusion



Introduction



Research



Model



Conclusion

# Challenge Summary



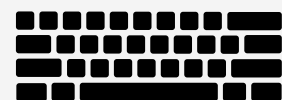
Navigate the EU AI Act by developing a chatbot.



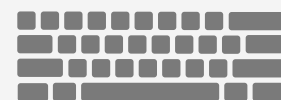
Specifically focuses on Natural Language Processing (NLP) and Retrieval-Augmented Generation (RAG) for a chatbot that understands the EU AI Act.



Implement a multi-agent approach for effective prompt engineering and risk assessment, ensuring the chatbot aligns with EU AI regulations.



Introduction



Research



Model



Conclusion



# Why is this Important?



This would help businesses understand and comply with these complex regulations, reducing compliance risks and promoting responsible AI development. This project is vital for ensuring your company's alignment with regulatory standards, and it offers students practical experience in AI regulation and multi-agent systems



Introduction



Research



Model



Conclusion



# Objectives

What do we want to achieve?



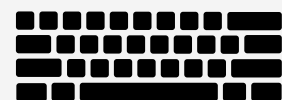
Successfully parse and extract relevant information from the EU AI Act PDF documents.



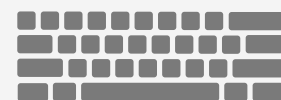
Develop a comprehensive knowledge base that the chatbot can use for informed decision-making.



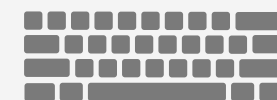
Design and implement a multi-agent system that enables the chatbot to provide accurate and context-aware advice.



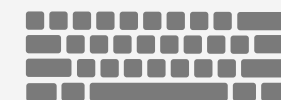
Introduction



Research



Model



Conclusion

# The EU AI Act

Search



The **EU AI Act**, proposed in April 2021, is the European Union's first major regulation aimed at governing artificial intelligence (AI) to ensure it is safe, transparent, and aligned with European values and human rights.

It introduces a risk-based approach, categorizing AI applications by levels of risk: unacceptable, high, limited, and minimal.

The Act aims to set a global standard for AI regulation, emphasizing ethics and accountability. The legislation will require companies to implement compliance measures, with penalties for non-compliance.

Save

Cancel



Introduction



Research



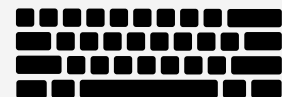
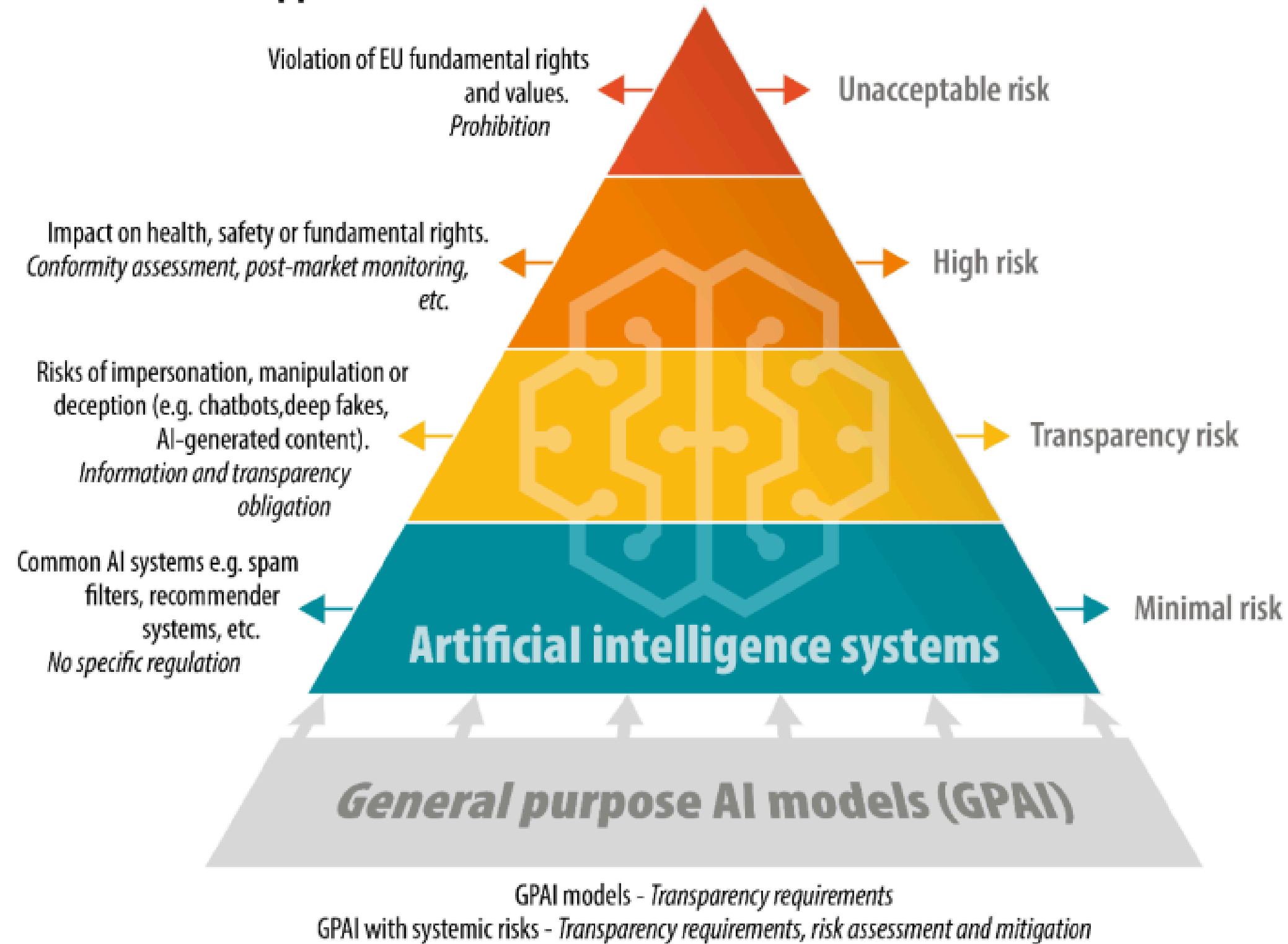
Model



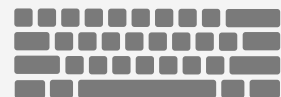
Conclusion



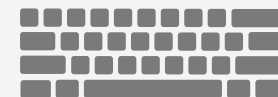
## EU AI act risk-based approach



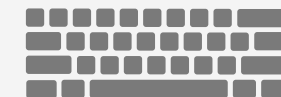
Introduction



Research



Model



Conclusion

# WHAT IS NLP and LLM?

Search



## NLP - Natural Language Processing



- NLP is a machine learning technology that allows computers to understand, interpret, and manipulate human language.

## LLM - Large Language Models

- LLM is a type of AI that can understand and generate human language.
- LLMs are trained on large amounts of data, such as text from the internet, and use deep learning techniques to perform NLP tasks.

Save

Cancel



Introduction



Research



Model



Conclusion

# WHAT IS RAG?

Search



## RAG: Retrieval-Augmented Generation



- It is a NLP technique that combines generative AI models with information retrieval systems.
- RAG improves the accuracy and relevance of text generated by LLMs by providing them with external knowledge.

Save

Cancel



Introduction



Research



Model



Conclusion

# WHAT IS spaCy?

Search



**spaCy** is an open-source library for Natural Language Processing (NLP) in Python.



## Our spaCy usage:

- Helps us with preprocessing text by removing stop words and punctuation.
- It performs tokenization (it create a list of token texts, excluding tokens that are stop words or punctuation.).

Save

Cancel



Introduction



Research



Model




Conclusion

# WHAT IS CohereAI?

Search



Cohere AI is an AI platform designed to help enterprises build powerful applications using natural language processing (NLP). 

## Key features about CohereAI that explain why we are using it:

- **Generative AI:** Cohere provides large language models (LLMs) that can generate human-like text, making it **useful for applications like chatbots**, content creation, and more.
- **Search and Discovery:** Their models are optimized for retrieving and ranking information accurately, which is helpful for search engines and recommendation systems.
- **Enterprise Solutions:** They offer tools for embedding, reranking, and **retrieval-augmented generation (RAG)**, which can be integrated into various business workflows.

Save

Cancel



Introduction



Research



Model



Conclusion

# Data Extration & Preprocessing

Search



## 1. Data Extraction

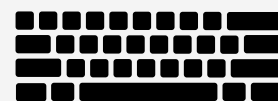
- **PDF Extraction Tool:** Used pdfplumber to load and extract text and tables from the PDF.
- **Content:** Retrieved structured (tables) and unstructured (text) data.

## 2. Text Exploration & Preprocessing

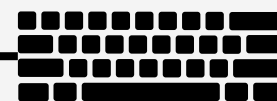
- **Tokenization:** Converted text to lowercase and removed special characters.
- **Stopword Removal:** Filtered out common stopwords for meaningful word frequency analysis.

Save

Cancel



Introduction



Research



Model



Conclusion



# Text Exploration & Preprocessing

Search



## 1. Word Frequency Analysis

- **Visualization**: Displayed top 10 most frequent words using a bar chart.

## 2. Sentiment Analysis

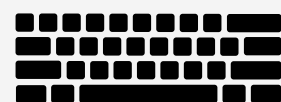
- **TextBlob**: Assessed sentiment polarity (positive/negative) and subjectivity.

## 3. Named Entity Recognition (NER)

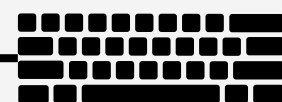
- **Entity Extraction**: Identified key entities (people, organizations, locations) with spaCy for deeper insights.

Save

Cancel



Introduction



Research



Model



Conclusion

# Building Model

Search



- **RAG Model**

- Retrieval

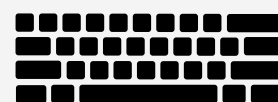
- Search engine
    - Scans database of document chunks
    - Find most relevant information

- Generation

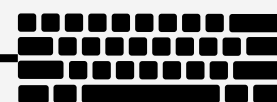
- Takes retrieved information and crafts a clear, meaningful response
    - Reply on Cohere's AL model

Save

Cancel



Introduction



Research



Model



Conclusion

# Tech Stack, Tools, and Techniques:

Search



- **Tools & Technologies:**

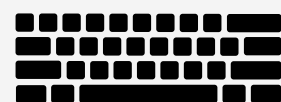
- [spaCy](#): clean and preprocessed text
- [hnswlib](#): Indexed documents into chunks
- [cohere's API](#): to generate responses that feel natural and informative

- **Techniques:**

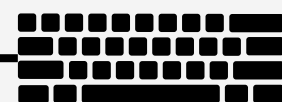
- [Text preprocessing](#): removed stop words, punctuation for clean inputs
- [chunking](#): split documents into smaller, manageable pieces
- [Embedding Generation](#): Turned text chunks into high-dimensional vectors
- [Vector Search](#): Found relevant chunks with approximate nearest neighbor search
- [RAG](#): combined retrieval with AL-generated responses for context-aware answers

Save

Cancel



Introduction



Research



Model

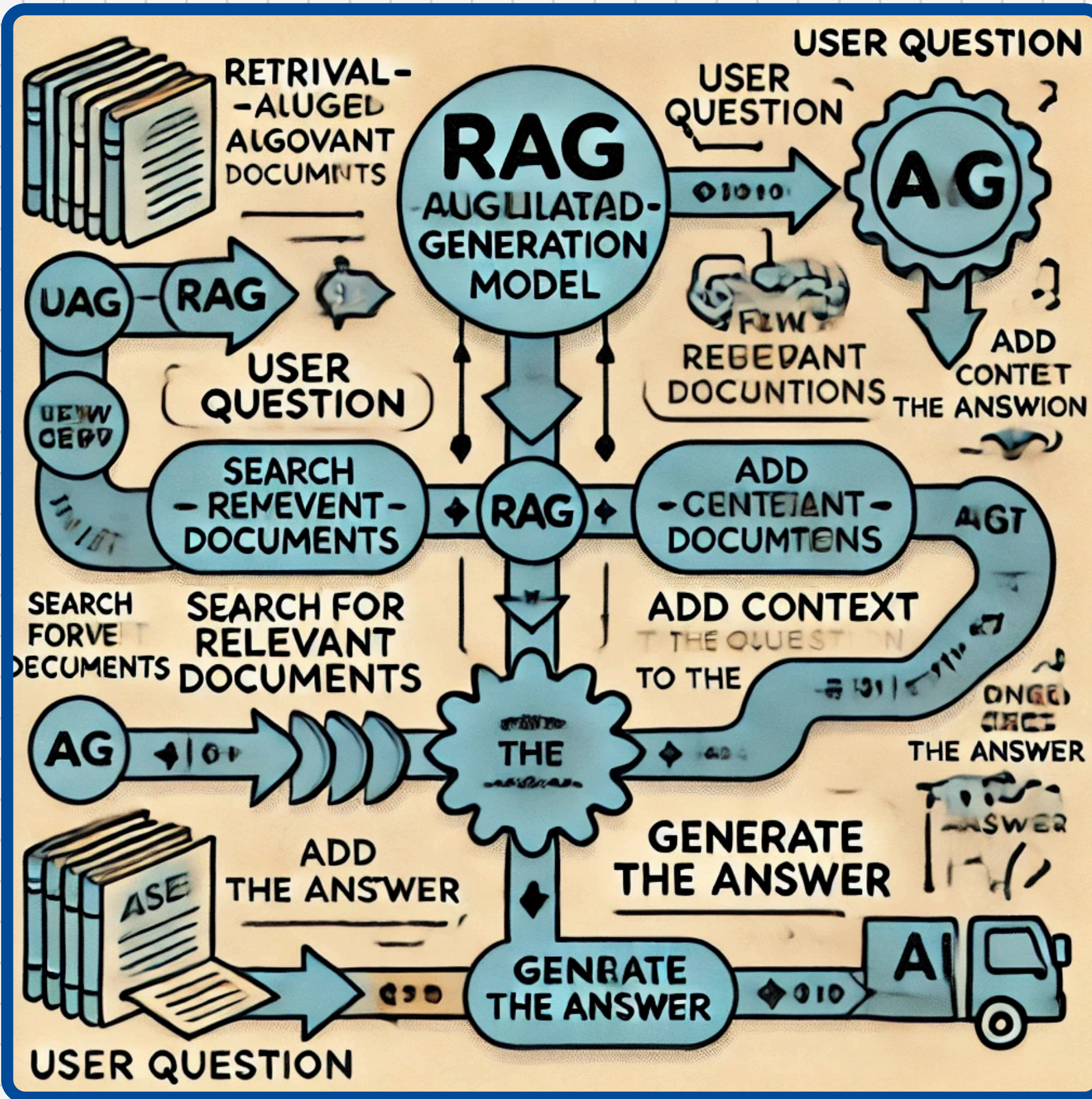


Conclusion



# Cycle Overview

1. User asks a question.
2. The system searches for relevant documents.
3. The RAG model combines the query with retrieved documents.
4. Context is augmented to make the question richer.
5. The AI generates an answer.





+ Code + Text

✓ RAM Disk Gemini ^

✓ [56] # Example query 1  
query = "What is the EU AI act?"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

✓ [57] # Example query 2  
query = "What is high risk and minimal risk?"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

✓ [58] # Example query 3  
query = "What is impact on health, safety, and fundamental rights considered for EU AI act?"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

✓ [59] # Example query 4  
query = "What is impact on health, safety, and fundamental rights considered?"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

✓ [60] # Example query 5  
query = "What year was the EU AI Act proposed?"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

✓ [61] # Example query 6  
query = "What year was the EU AI Act passed?"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

✓ [50] # Example query 7  
query = "Explain the EU AI act risk-based approach"  
response\_text = chatbot\_query(query, vectorstore)  
print(response\_text)

↑ ↓ ↻ 🔗 ⚙️ 📄 🗑️ ⋮

# Evaluation of Model

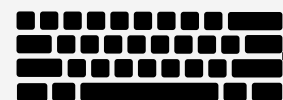
Search



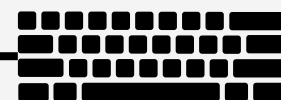
- **Model:**
  - Strong in accuracy but lags in detail, structure, and contextual clarity
- **ChatGPT:**
  - Provides clear, detailed, and easy-to-understand answers that cover all the important points while adding thoughtful insights for a deeper understanding.

Save

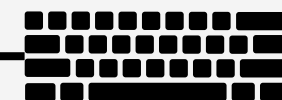
Cancel



Introduction



Research



Model



Conclusion



# Model Output Comparison:

Search



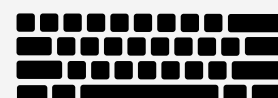
**Prompt:** What is the EU AI Act?

**Our models response:** The EU AI act is a draft artificial intelligence (AI) act that sets a common framework for the use and supply of AI systems in the EU. It offers a classification of AI systems and defines general-purpose AI systems as systems based on a GPAI model with the capability to serve a variety of purposes through direct use or integration with other AI systems. The act applies primarily to providers and deployers of AI systems and GPAI models who put these systems into service or place them on the EU market.

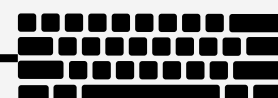
**ChatGPT response:** The EU AI Act is the world's first binding horizontal regulation on artificial intelligence, proposed by the European Commission in April 2021. It sets a common framework for the use and supply of AI systems in the EU. It classifies AI systems by risk levels and establishes requirements tailored to each category, ranging from prohibited practices to minimal-risk systems.

Save

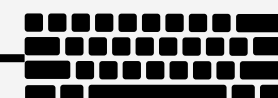
Cancel



Introduction



Research



Model



Conclusion

# Challenges



Pinpointing most effective AI techniques and Python libraries



Breaking down the document in a meaningful way



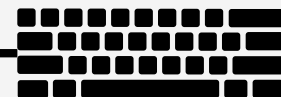
Translating course material and applying to this problem



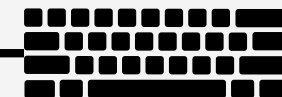
Communication and collaboration asynchronously



Introduction



Research

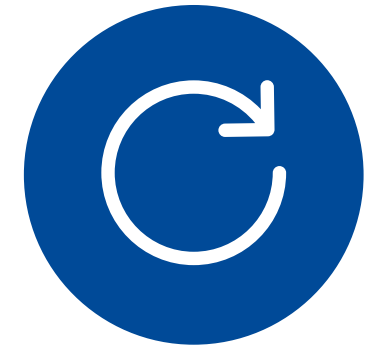


Model



Conclusion

# Insights & Learnings



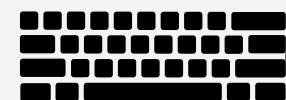
Working on an  
AI project

Collaborative  
development  
with tools like  
Git and Notion

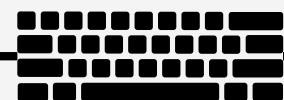
RAG framework

EU AI Act

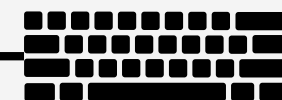
Choosing AI  
model



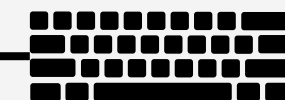
Introduction



Research



Model



Conclusion



# Thank You

**Any questions?**

