Vectice White Paper

The EU AI Act

Documentation is <u>no longer</u> optional

The AI Act's impact on EU businesses and the urgency to safeguard their AI future

In this white paper:

EU AI Act: First Regulation on Artificial Intelligence

The AI Act's Impact on Businesses

The Regulatory Horizon

Moving Towards AI Compliance

The Vectice Solution - Auto-documentation for AI you trust, faster

vectice

March 2024

Introduction

EU AI Act: First Regulation on Artificial Intelligence

The introduction of the EU AI Act has triggered a pressing need for businesses to align with new AI regulations, specifically the stringent technical documentation requirements for high-risk AI systems. Meeting these demands poses substantial challenges in documentation consistency, team alignment, and accountability.

As part of its digital strategy, the EU wants to regulate AI to ensure better conditions for the development and use of this innovative technology.

In this white paper:

1. EU AI Act: First Regulation on Artificial Intelligence

What is the EU AI Act?

The AI Act is a proposed European law on artificial intelligence (AI) and was passed on March 13th, 2024 – the first law on AI by a major regulator anywhere. The law assigns applications of AI to three risk categories:

- First, applications and systems that create an unacceptable risk, such as government-run social scoring of the type used in China, are banned.
- Second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements.
- Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.

Key Deadlines Post-EU AI Act Publication

The publication of the AI Act in the EU's Official Journal is anticipated to occur between May and July; 20 days after publication, the Act officially becomes effective.

- 6 months after the Act becomes effective: Prohibitions will be active.
- 12 months after the Act becomes effective: Governance guidelines and responsibilities for general-purpose AI models will kick in.
- 2 years after the Act becomes effective: The Act will be completely enforceable.
- 36 months after the Act becomes effective: Regulations for AI systems integrated into regulated products will be enforced.

Growing Scope of 'High-Risk AI Systems' under the AI Act

The AI Act has a broad scope and affects various stakeholders involved in AI development and use. It applies to businesses within the EU (regardless of size and industry) and extends to entities outside the EU serving EU citizens.

High-Risk AI Systems

High-risk AI systems must meet specific legal requirements and undergo assessment before being allowed on the market. The Commission holds the authority to define the list of high-risk AI systems subject to regulation.

This list can be extended in the future without the necessity of an additional vote! ⚠️

2. The AI Act's Impact on Businesses

To meet the challenge of the AI Act, businesses and organizations need to be prepared with the necessary technical end-to-end documentation of the entire model lifecycle; including the techniques, procedures, and systematic actions to be used during the design, control, and verification stages of these systems.

a.   **Technical Documentation**
b.   **Top 3 Challenges In Achieving Documentation Compliance**
c.   **Failing to Comply**

2.a Requirement for Comprehensive Lifecycle Documentation

Under the AI Act, businesses are required to establish comprehensive technical documentation that covers the entire lifecycle of their AI models. This makes the need for end-to-end documentation mandatory for any entity operating in EU countries.

Two articles within the AI Act sheds light on the specific documentation requirements for high-risk AI systems:

- Article 15, Paragraph 2: The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

- Article 17, paragraph 1: Providers of high-risk AI systems must establish a documented quality management system to comply with this Regulation, including: **(b)** techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system; **(c)** techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system.

The technical documentation should encompass aspects such as development, production, and monitoring, with a particular focus on the datasets used. According to the act, technical documentation for a high-risk AI system must be prepared before it is launched or deployed, and this documentation must be regularly updated (Article 11). Nevertheless, this undertaking presents numerous challenges for modeling teams.

2.b Top 3 Challenges in Achieving Documentation Compliance

Complying with documentation requirements (Art. 15 and Art. 17) poses challenges for modeling teams. One of the primary hurdles is the historical struggle of modeling teams to effectively document their work. **Documentation often takes a backseat to the urgency of delivering results**, leading to incomplete or insufficient records of the design, development, and quality control processes of high-risk AI systems.

1. **Unifying Documentation Across Diverse Tools and Platforms**

    Unifying documentation across diverse tools and platforms complicates compliance. Different software, frameworks, and languages generate their own formats, hindering consolidation and presentation of cohesive documentation.

2. **Achieving Alignment in Documentation Practices Across Diverse Teams**

    Achieving alignment in documentation practices across diverse teams is challenging. With members from various backgrounds, inconsistencies and gaps in documentation may arise. Establishing clear guidelines and standards is crucial.

3. **Addressing Documentation Challenges for High-Risk AI Systems**

    Addressing documentation challenges for high-risk AI systems requires prioritizing documentation efforts, setting guidelines, and investing in tools for seamless integration. Overcoming these hurdles ensures transparency, accountability, and compliance with regulations.

2.c Failing to Comply

Failure to comply with the documentation requirements outlined in the European AI Act carries significant consequences.

Businesses may face hefty **7% of a company's global revenue that's 75% higher than GDPR infringements.** It is imperative for companies to recognize that documentation is no longer optional but an essential component of responsible and compliant AI deployment.

3. The Regulatory Horizon

Countries across the globe are currently at different stages in their efforts to establish effective regulations for artificial intelligence (AI). These countries hold divergent perspectives on the most suitable methods for governing AI:

   a.   **AI Regulation Around The World**
   b.   **Unified Regulatory Direction**

3.a AI Regulation Around the World

Several countries, including the United States, China, Canada, India, and the United Kingdom, have taken notable steps towards regulating artificial intelligence (AI) and shaping policies in this domain. Each country has developed its own approach, ranging from proposed bills and blueprints to pro-innovation strategies. Below is a summary of the mentioned countries and their strategies of regulating AI:

- **United States of America** - Blueprint for an AI Bill of Rights
- **China** - Next Generation Artificial Intelligence Development Plan
- **Canada** - Artificial Intelligence & Data Act (AIDA)
- **India** - Digital India bill
- **United Kingdom** - Pro-innovation approach to AI Regulation

3.b Unified Regulatory Direction

While certain AI developers and technology industry leaders propose a six-month pause on the development of Large Language Model AI to enable regulation to catch up, it appears improbable that a **consensus will be swiftly reached regarding the optimal approach to regulating AI.** Striking a balance between fostering innovation and mitigating the potential risks associated with AI remains a complex challenge.

Key Takeaways From The AI Act

- The EU AI Act is certainly coming and robust end-to-end documentation will no longer be optional.

- **Comprehensive model documentation stands as a strategic and fundamental aspect for ensuring the ongoing delivery of responsible AI solutions.**

- Failure to comply with documentation requirements risks substantial financial penalties and undermines transparency, accountability, and public trust in AI.

- The list of regulated **use-cases is expected to expand over time** and can be passed by the European Parliament without vote.

4. Moving Towards AI Compliance

The EU's rollout of the new AI Act is causing a shift in AI application and advancement. This entails broader participation from various stakeholders in AI initiatives, coupled with traceability of decisions being taken and establishment of safeguards. Enhanced engagement with non-technical experts, such as those in legal and business domains, is now crucial.

What this means for businesses operating in the EU:

- Upcoming regulations center around AI models, requiring distinct teams to oversee compliance compared to those managing GDPR-related matters.
- The involvement of more stakeholders requires careful decision tracking and the implementation of safeguards.
- Effective oversight of decision-making and model explainability is imperative.
- Model teams must now not only train models, but also communicate critical insights to non-technical stakeholders such as business and legal teams.

Ensuring responsible and well-regulated AI starts with documentation of models. Two distinct approaches have surfaced, each with its implications:

Manual Documentation:	Auto-Documentation:
Manually documenting models comes with a heavy workload and expenses, exemplified in sectors like banking where costs can soar to a substantial **USD 50 million**, highlighting its significant impact.	Specialized documentation software like Vectice can automate repetitive documentation tasks. This reduces the manual effort required and increases the robustness with low risk and lower cost.

Auto-documentation for AI you trust, faster

By adopting Vectice, businesses can ensure compliance with regulatory requirements, manage the increasing complexity of AI models, and maintain transparency, accountability, and public trust in AI-powered services.

Why businesses must act now:
- Increasing model complexity
- Rapidly growing and changing regulations
- Regulation and compliance is expensive and the right interface becomes strategic
- High-risk AI application use-cases can expand at any time

The Vectice solution:
- Automated Documentation of the end-to-end model lifecycle
- Cross-functional place where model teams, business stakeholders, governance, legal and risk teams can work together
- Cross-functional approval workflows & guardrails for responsible AI
- Enhanced transparency & visibility for all stakeholders

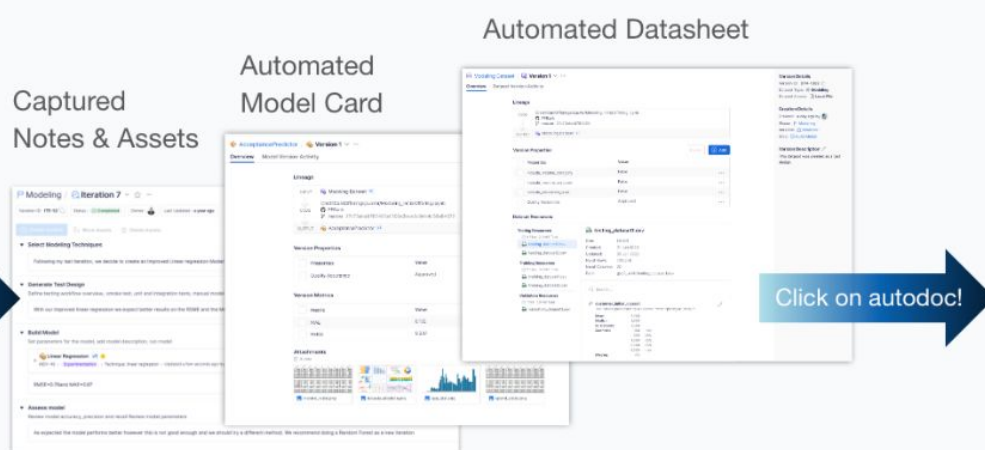## No matter your stack, get started with vectice today!

Instant acceleration of your analysis/model to production

✓ Most automated documentation solution   ✓ Optimized for data science & AI workflows: interactive, exploratory

✓ Works with **any stack** in **Python** or **R**

✓ Including **MLflow, VertexAI, Comet ML** to document current & past work

By utilizing Vectice as a model documentation solution, businesses can effectively address the documentation challenges posed by the EU AI Act.

Vectice streamlines compliance efforts, ensures comprehensive and accurate documentation, and provides the necessary tools and workflows to navigate the regulatory landscape in a responsible and compliant manner.

Try Vectice for free

www.vectice.com
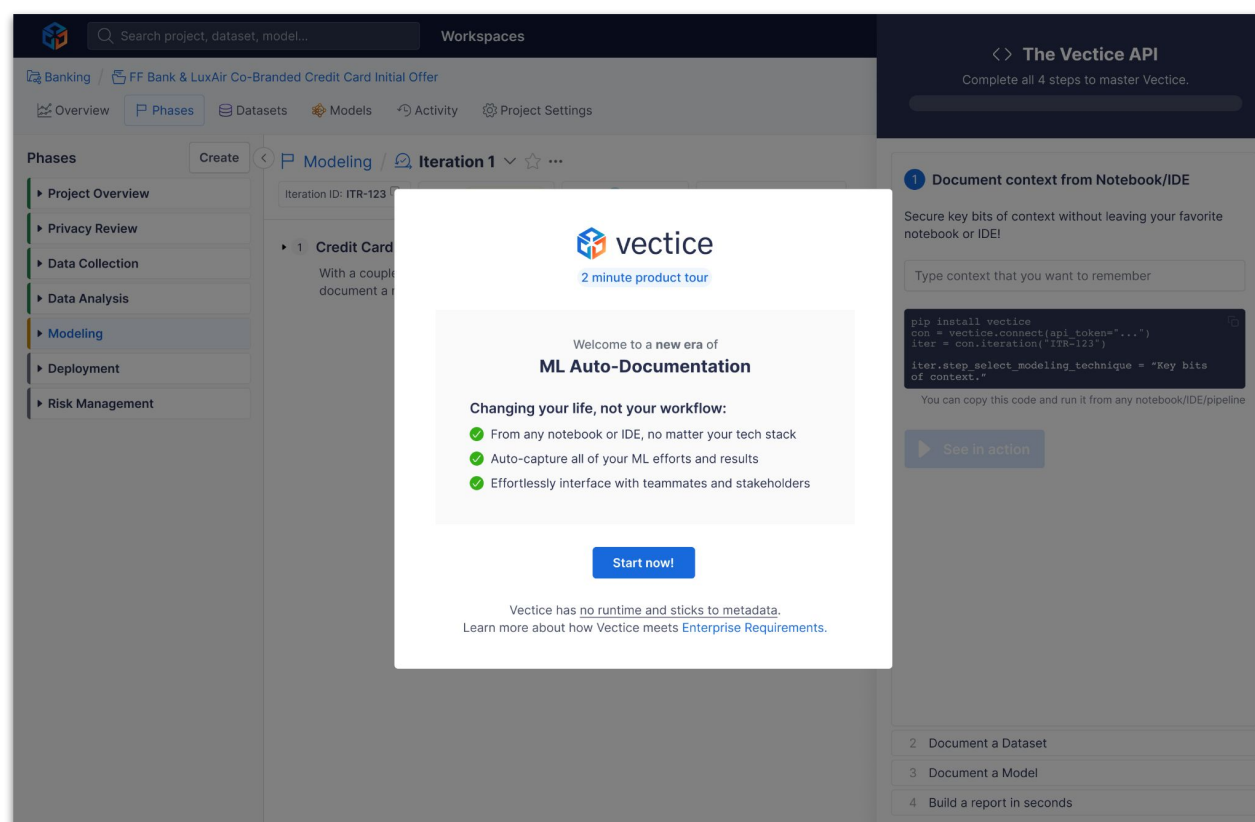
Learn more about Vectice and how it can support you

785 Market Street, Suite 700, San Francisco CA 94103 - United States

✉ contact@vectice.com   📞 (650) 399 - 0114