Scrut Automation

Seven Focus Areas to Navigate The EU AI Act

Introduction

The EU AI Act is a landmark legislation that aims to curb the potential harm of AI while supporting innovation and promoting a human-centric approach to its development and use. That said, it is very broad in its scope, and it can be difficult to know where to begin.

This guide is ideal for startup founders looking to work with and develop AI systems in the European Union as it highlights the seven focus areas towards building secure, transparent, and ethical AI systems.

The key here is to mitigate the risks from high-risk AI systems. Let's take a look at these focus areas below:

Focus Area 1:
Implementing Risk and Quality Management Systems

The EU AI Act is like the ultimate safety net for high-risk AI systems, making sure nothing slips through the cracks from start to finish. It aims to identify and assess risks to health, safety, and fundamental rights, whether from intended use or potential misuse. This includes thorough risk evaluations, targeted solutions to reduce risks, and detailed documentation.

- **Identify and analyze risks:** Stay ahead by spotting potential risks to health, safety, and rights throughout the AI system's life. This covers both how it's meant to be used and any possible misuse.
- **Estimate and evaluate:** Gauge how likely and severe those risks are, whether from intended use or misuse, using data from post-market monitoring.
- **Mitigate risks:** Put the right risk management measures in place based on how serious the risks are, with targeted solutions to tackle each issue.
- **Document everything:** Keep detailed records of the whole process, from risk assessments to actions taken, as required by the AI Act.

Note to startups: The EU AI Act mentions conducting periodic reviews and updates to ensure the risk management system remains effective. This includes revisiting the risk assessment when relevant factors change.

Focus Area 2:
Having An Effective Data Governance Program in place

The AI EU Act emphasizes the need for high-quality data in AI systems, ensures compliance with data protection laws, and addresses bias in relation to the target population. It also mandates transparency about how and why data is collected.

- **Use reliable data sets:** Make sure your data sets are relevant, complete, and error-free for the AI's intended purpose, from training to testing, while considering biases that might affect outcomes.
- **Mitigate bias:** Focus on identifying and reducing biases in your data to avoid discrimination, especially in areas like health, safety, or fundamental rights where AI decisions have a real impact.
- **Maintain high data standards:** Track where your data comes from and its quality, ensuring clear processes for acquiring, analyzing, storing, and managing it, to support transparency and accountability.
- **Be clear about data usage:** Clearly communicate the purpose behind data collection, particularly when dealing with personal data, following data protection laws.

Note to startups: The EU AI Act mentions considering using third-party certified compliance services to verify data governance practices.

Focus Area 3:
Having Detailed Technical Documentation in Place

Thorough documentation for high-risk AI systems, as mandated by the AI EU Act, includes details about the system's design, development, and performance. It must also cover information on algorithms, data used, training processes, risk management, and clear user instructions on the system's capabilities, limits, and potential risks.

- **Maintain comprehensive documentation:** Prepare and maintain detailed technical documentation that demonstrates compliance with the AI Act's requirements. This documentation should also be accessible, and understandable.
- **Provide clear and concise instructions:** These instructions should enable deployers to understand the system's capabilities, limitations, and risks. Instructions for use should include information on performance metrics, potential risks, and human oversight measures.
- **Make sure to have the necessary information for authorities:** Ensure the technical documentation includes information necessary for national competent authorities and notified bodies to assess compliance. This includes details on the AI system's design, development, and testing processes.
- **Keep documentation up-to-date:** Continuously update the technical documentation to reflect any changes or modifications made to the AI system. This ensures the documentation remains accurate and relevant throughout the AI system's lifecycle.

Note to startups: The EU AI Act mentions that Small and Medium Enterprises startups can use a simplified technical documentation form for this purpose.

Focus Area 4:
Maintain Transparency Across Your AI System

The EU AI Act emphasizes transparency in high-risk AI systems so that users can make informed decisions and be accountable for their use. This means providing easily accessible information about how the AI system works, including its strengths and weaknesses. The design should allow users to understand the AI's internal mechanisms and effectively evaluate its performance.

- **Inform users about AI interaction:** Notify individuals when they are interacting with an AI system unless it is obvious from the context. The notification should be clear, distinguishable, and provided at the latest during the first interaction.
- **Mark synthetic content:** Implement technical solutions to mark synthetic audio, image, video, or text content as artificially generated or manipulated. This requirement aims to prevent the spread of disinformation and protect the authenticity of content.
- **Be transparent about your AI System's capabilities and limitations:** Provide clear and accessible information to users about the AI system's capabilities, limitations, and foreseeable risks. The information provided should be meaningful and comprehensive, taking into account the target audience.

Note to startups: The EU AI Act mentions designing high-risk AI systems so that deployers can understand how the system works and evaluate its performance

Focus Area 5:
Ensuring Accuracy, Robustness, and Cybersecurity of AI Systems

The EU AI Act has strict requirements for high-risk AI systems to ensure they perform consistently and can withstand errors, malfunctions, or attacks. Strong cybersecurity measures are crucial to protect the system's integrity and prevent unauthorized access or tampering.

- **Maintain consistent performance:** Ensure the AI system performs consistently and accurately throughout its lifecycle, in line with its intended purpose. This involves setting appropriate performance metrics and evaluating the system's accuracy and robustness.
- **Ensure resilience to errors and attacks:** Design and develop the AI system to be robust and resilient against errors, faults, inconsistencies, and adversarial attacks. Cybersecurity measures should be implemented to protect against unauthorized access and data breaches.
- **Adopt robust cybersecurity measures:** Implement appropriate cybersecurity measures to protect the AI system from unauthorized access, data breaches, and malicious attacks. The system should be designed to be resilient against cybersecurity threats, ensuring the integrity and confidentiality of data.

Note for Startups: The EU AI Act mentions considering compliance with the Regulation on horizontal cybersecurity requirements for products with digital elements for demonstrating cybersecurity compliance.

Focus Area 6:
Have a Post-Market Monitoring System in Place

Continuous monitoring of high-risk AI systems after deployment involves collecting, documenting, and analyzing data from users and other sources to ensure the system meets the EU AI Act's requirements. Any serious incidents must be reported to market surveillance authorities.

- **Monitor system performance:** Establish a system for monitoring the AI system's performance and compliance after it has been placed on the market or put into service. This involves collecting, documenting, and analyzing system performance data to ensure continuous compliance.
- **Report serious incidents:** Report any serious incidents or malfunctions that result in harm to health, safety, fundamental rights, property, or the environment to the relevant authorities. This includes notifying market surveillance authorities about incidents and following established reporting procedures.
- **Gather data and improve:** Use post-market monitoring data to identify areas for improvement and update risk management and quality systems. Continuous monitoring allows for system enhancements and ensures ongoing compliance with regulatory requirements.

Note to startups: The EU AI Act notes that post-market monitoring should not include sensitive operational data of law enforcement authorities.

Focus Area 7:

Establishing Adequate Human Oversight Of AI Systems

The EU AI Act emphasizes the importance of human oversight for high-risk AI systems to ensure that humans remain in control of AI operations and can intervene when necessary to prevent or mitigate potential harm. The Act also requires incidents involving high-risk AI systems to be reported within a specific timeframe, typically 15 days, with non-compliance potentially leading to severe penalties.

- **Ensure Effective human oversight:** Design the AI system to allow for effective human oversight throughout its operational phase. These might include having in-built operational constraints that the system itself cannot override, and having mechanisms for human intervention to avoid negative consequence
- **Placing competent human operators as part of the oversight:** Ensure human operators have the necessary competence, training, and authority to understand and respond to the AI system's operations. Human operators should have appropriate training in AI literacy and the specific system they oversee.

Note to startups: The EU AI Act mentions providing human operators with appropriate tools and mechanisms to intervene in the AI system's operation and address any anomalies or risks. This includes providing tools for monitoring, interpreting outputs, and taking corrective actions.

There you have it: The seven focus areas of the EU AI Act's requirements for contributing to a responsible and ethical AI landscape. Remember, the EU AI Act is a complex regulation, and this list provides a high-level overview. Startups are encouraged to consult with legal experts and stay updated on the latest developments.

For more information and expert advice on any of these focus areas, contact Scrut Automation today!