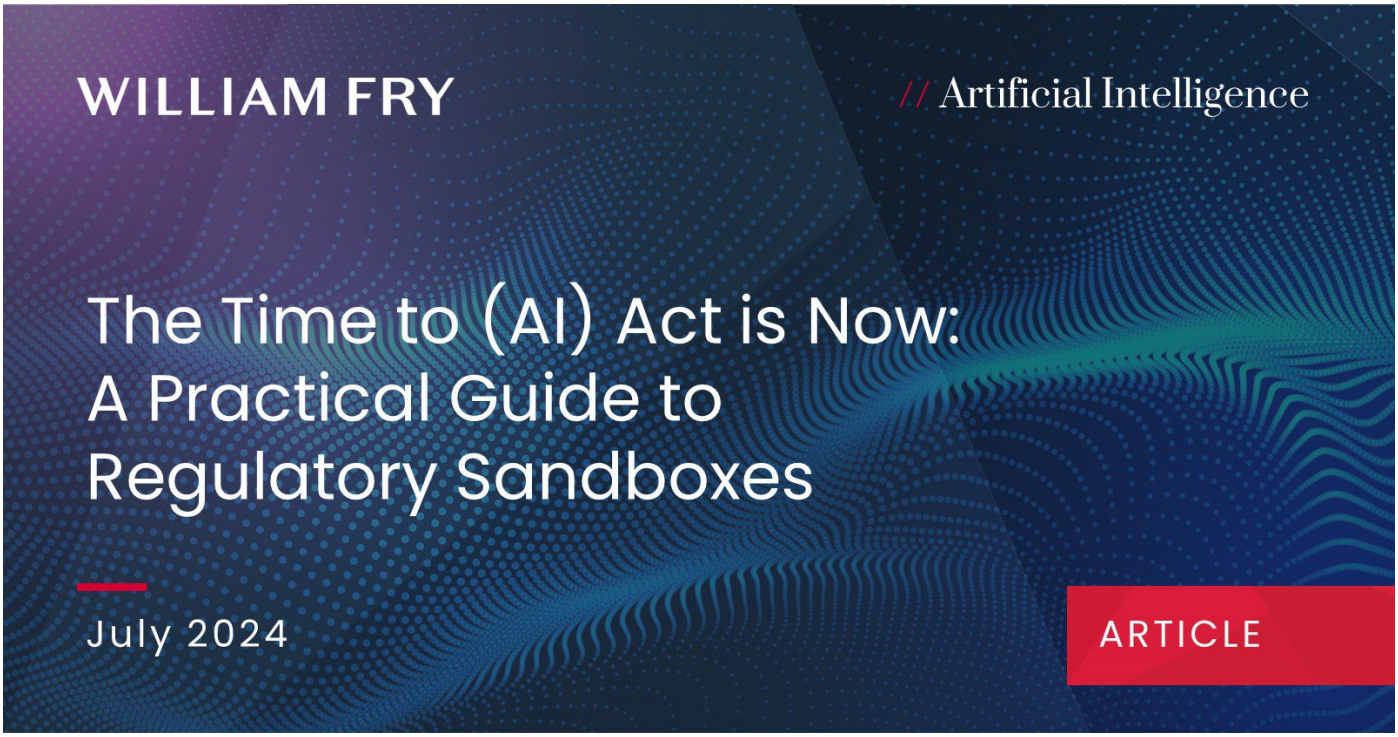
The Time to (AI) Act is Now: A Practical Guide to Regulatory Sandboxes Under The AI Act

July 24, 2024



The European Union's AI Act represents a significant step forward in the regulation of artificial intelligence (AI) technologies, particularly concerning the use of emotion recognition systems.

These systems, which infer or identify emotions from biometric data, pose unique challenges and risks that necessitate strict regulatory measures.

A. Overview Regulatory Sandboxes in the AI Act

Within the AI Act, regulatory sandboxes are defined as frameworks established by competent authorities. These frameworks allow providers or prospective providers to test innovative AI systems in real-world conditions for a limited period. The operation of these sandboxes is governed by a "sandbox plan," which details the objectives, conditions, timeframe, methodology, and requirements for the activities conducted within the sandbox. This plan is a mutually agreed document between the AI provider and the competent authority, ensuring clear guidelines and expectations for the testing phase.

The Act mandates that each Member State must establish at least one AI regulatory sandbox at the national level within 24 months of the regulation's entry into force. These

sandboxes may also be established jointly with other Member States or by participating in existing sandboxes, provided they offer an equivalent level of national coverage. Additionally, Member States can establish further sandboxes at regional or local levels or in cooperation with other Member States.

The European Data Protection Supervisor may also establish an AI regulatory sandbox specifically for EU institutions and bodies. To support the effective and timely operation of these sandboxes, Member States must allocate sufficient resources and ensure cooperation among relevant authorities. These sandboxes provide a controlled environment to facilitate the development, training, testing, and validation of AI systems before their market deployment, following a specific sandbox plan agreed upon by the involved parties.

Competent authorities are tasked with providing guidance, supervision, and support within the sandbox. This includes identifying and mitigating risks, particularly those related to fundamental rights, health, and safety. Authorities also issue documentation and exit reports, which detail the activities and outcomes of the sandbox testing. These reports can be used by providers to demonstrate regulatory compliance.

The Commission and the AI Board have the authority to access exit reports to aid in their regulatory tasks. The establishment of AI regulatory sandboxes aims to improve legal certainty, support the sharing of best practices, foster innovation, facilitate regulatory learning, and enhance market access for small and medium-sized enterprises (SMEs) and start-ups. When personal data processing is involved, data protection authorities must be included in the sandbox operation.

Competent authorities retain supervisory powers and can suspend sandbox activities if significant risks are identified. Participants remain liable under applicable laws but may be exempt from administrative fines if they adhere to the sandbox plan and follow the guidance provided by authorities in good faith. The framework is designed to facilitate cross-border cooperation among national authorities and ensure coordination within the AI Board framework.

The AI Office is responsible for maintaining a public list of sandboxes to encourage interaction and cooperation. National authorities must submit annual reports on the progress, incidents, best practices, and outcomes of their sandboxes to the AI Office and Board. These reports help inform regulatory practices and may lead to adjustments in the regulatory framework.

The Commission will develop detailed arrangements for the establishment and operation of sandboxes through implementing acts. These acts will specify eligibility and selection criteria, procedures for application and participation, and terms and conditions for participants. Sandboxes must ensure fair and transparent access, particularly for SMEs and start-ups, and facilitate the involvement of various stakeholders in the AI ecosystem.

Personal data collected for other purposes may be processed within sandboxes under

specific conditions, primarily when developing AI systems for substantial public interest. This processing must comply with data protection laws, and data should be handled in a separate, protected environment with appropriate safeguards.

Providers can also test high-risk AI systems in real-world conditions outside sandboxes, provided they meet specific conditions and obtain necessary approvals. This testing must ensure informed consent from participants, and providers must implement measures to protect participants' rights and safety.

The AI Act prioritises support for SMEs and start-ups by ensuring they have priority access to sandboxes and tailored support services. Member States are encouraged to establish communication channels and provide guidance to SMEs throughout their development. The Commission will support these efforts by providing standardised templates and maintaining an information platform for stakeholders.

B. Key Dates:

12 July 2024: The AI Act published in the Official Journal.

1 August 2024: The AI Act will become law.

2 August 2026: Member States' competent authorities will need to have established at least one AI regulatory sandbox at national level.

Annual Reporting: Member States must submit annual reports to the AI Office and the Board starting one year after the establishment of the sandboxes.

C. Enforcement and Penalties

Competent authorities have the power to supervise, guide, and support participants within the sandboxes. They are tasked with identifying and mitigating risks, particularly those affecting fundamental rights, health, and safety. If significant risks are detected and cannot be effectively mitigated, authorities can suspend or terminate the testing process within the sandbox.

Article 57(12) specifies that providers participating in sandboxes remain liable for any damage caused to third parties. However, if they adhere to the sandbox plan and act in good faith following the guidance of the competent authorities, they are shielded from administrative fines under the AI Act.

D. Steps to Compliance:

1. Understand the AI Act: Familiarise yourself with the AI Act's requirements and the specific obligations for your AI system based on its risk classification.

2. Participate in Sandboxes: Engage with national competent authorities to participate in AI regulatory sandboxes. This involves preparing a sandbox plan (Article 3(54)) that outlines objectives, conditions, timeframes, and methodologies for sandbox activities.

3. Follow Guidelines: Adhere to the guidance and supervision provided by competent authorities. This includes implementing risk mitigation measures and maintaining detailed records of testing and validation activities.

4. Annual Reporting: Comply with reporting obligations by submitting required documentation and reports to competent authorities, the AI Office, and the Board.

5. Exit and Conformity Assessment: Upon successful completion of sandbox activities, utilise the exit report and written proof provided by competent authorities to streamline the conformity assessment process for market entry.

The AI Act represents a significant step forward in regulating AI within the European Union, ensuring that innovation does not come at the expense of safety and fundamental rights. Regulatory sandboxes are a cornerstone of this framework, offering a controlled environment for developing and testing AI systems. By understanding the requirements and leveraging the support offered through sandboxes, AI providers can navigate the regulatory landscape effectively, fostering innovation while ensuring compliance. The establishment of these sandboxes, alongside stringent oversight and guidance, aims to create a robust and innovative AI ecosystem within the EU.

For further guidance and support on AI compliance, please contact Barry Scannell, Leo Moore, Rachel Hayes, or any member of the William Fry Technology Department.