IBA/IFA 40th
ANNUAL JOINT CONFERENCE

* * * * *

The Future of Global Franchising: Innovations, Technologies, and New Markets

* * * * *

NEWS FROM AROUND THE WORLD
The European Union Artificial Intelligence Act: Legal Analysis and Implications

•

May 7, 2025
Washington, D.C. U.S.A.

Olivia GAST
Gast Avocats & Mediation
Paris, France

Table of Contents

1. Introduction

The **EU Artificial Intelligence Act (EU AI Act)**, formally known as **Regulation (EU) 2024/1689**, was officially published on **12 July 2024** and entered into force on **1 August 2024**. This legislation marks a landmark achievement in regulating artificial intelligence (AI) across the European Union, establishing the first comprehensive legal framework aimed at ensuring that AI technologies are safe, transparent, and consistent with European values, particularly human rights and ethical standards (Recital 1, Regulation (EU) 2024/1689).

The Act adopts a **risk-based approach** to regulate AI systems, categorizing them according to the level of risk they pose to individuals and society. By addressing these risks proportionately, the Act strives to foster innovation while safeguarding fundamental rights, such as privacy and non-discrimination, as guaranteed under the **EU Charter of Fundamental Rights** (Article 1, EU Charter).

While the Act entered into force in August 2024, the majority of its provisions will be fully enforceable by **2 August 2026**, marking the end of the transition period. This paper provides an in-depth legal analysis of the key provisions within the **EU AI Act**, including its **governance framework**, **compliance obligations**, and **risk classification system**. It also explores the implications of the Act for franchise networks, with a specific focus on the legal challenges and opportunities presented by AI use.

2. Definition of AI under the EU AI Act

2.1 AI as Defined in the Regulation

One of the foundational aspects of the **EU AI Act** is the definition of AI systems, provided in **Article 3(1)** of Regulation (EU) 2024/1689. The regulation defines AI as “machine-based systems that are designed to

operate with varying levels of autonomy and may exhibit adaptiveness after deployment." These systems are capable of making predictions, recommendations, decisions, or generating content that impacts both physical and virtual environments.

This broad and flexible definition ensures that the regulation remains relevant as AI technologies evolve. It draws on international definitions, such as those from the **Organisation for Economic Co-operation and Development (OECD)**, to establish a comprehensive framework that addresses both current and future AI applications. The definition is critical for the purposes of legal compliance, as it determines what constitutes an AI system under the regulation and helps avoid ambiguities in enforcement.

2.2 Key Concepts for Legal Frameworks

The legal significance of this definition lies in providing clarity and certainty for the regulation of AI systems. The definition is intentionally broad to cover the diverse range of AI technologies, ensuring that both developers and users understand their legal obligations. In particular, the regulation emphasizes key legal concepts such as **accountability**, **liability**, and **transparency**.

Like the **General Data Protection Regulation (GDPR)**, which governs data processing in the EU, the **EU AI Act** stresses the importance of ensuring that AI systems respect fundamental rights. For instance, **Article 5** of the AI Act mandates that AI systems should not be used for "unacceptable risk" purposes, such as social scoring or the manipulation of vulnerable individuals (Article 5, Regulation (EU) 2024/1689).

3. Risk-Based Approach and Categories

The EU AI Act introduces a **risk-based framework** that classifies AI systems into four categories: **unacceptable risk**, **high-risk**, **transparency risk**, and **minimal or no-risk**. This risk-based classification allows for a proportionate regulatory approach that tailors obligations based on the potential harm an AI system could cause.

3.1 Unacceptable Risk AI Systems

As per **Article 5**, certain AI systems are classified as presenting an **unacceptable risk** and are thus prohibited. These systems include those that pose significant harm to individuals' rights, safety, and freedoms. Examples include AI used for:

- **Social scoring** by public authorities (Article 5(a)).
- **Predictive policing** based on biased algorithms (Article 5(b)).
- **Real-time biometric identification** in public spaces without consent (Article 5(c)).

These prohibitions aim to preserve **fundamental rights**, such as privacy and non-discrimination, in accordance with the **EU Charter of Fundamental Rights** (Articles 7 and 21, EU Charter). The legal framework sets clear boundaries for AI use that directly impacts individuals' freedoms and dignity.

3.2 High-Risk AI Systems

AI systems that present a significant risk to individuals' health, safety, or fundamental rights fall under the **high-risk** category, as defined in **Article 6** and **Annex III** of the AI Act. These include AI used in:

- **Critical infrastructure** (transportation, healthcare, energy).
- **Healthcare** (e.g., diagnostic AI tools).
- **Law enforcement** (e.g., AI in predictive policing or risk assessments).

High-risk AI systems are subject to stringent requirements such as **human oversight**, **data quality assessments**, and **risk mitigation strategies** (Article 6). Legal professionals will be tasked with ensuring

that businesses and public authorities comply with these strict obligations, especially in high-stakes areas like healthcare and law enforcement.

3.3 Transparency Risks

Transparency in AI operations is another core element of the regulation, as laid out in **Article 11**. AI systems that interact with humans must disclose their nature and purpose. This includes systems like chatbots or content generators, which should be clearly identified as AI-driven rather than human-operated. For example, generative AI models must ensure that any content they produce is easily identifiable as AI-generated (Article 11, Regulation (EU) 2024/1689).

Legal professionals will need to advise clients on how to meet these transparency obligations, ensuring that users are aware when they are interacting with AI systems and not human agents.

3.4 Minimal or No-Risk AI Systems

AI systems classified as **minimal or no-risk** are not subject to additional regulatory requirements beyond general legal frameworks like **consumer protection** or **data privacy laws**. These systems include AI applications such as **spam filters** or **video games** (Article 3, Regulation (EU) 2024/1689).

However, developers of these systems are encouraged to voluntarily apply the **Trustworthy AI** principles outlined in the Act. For example, businesses could voluntarily commit to ensuring that their minimal-risk AI systems align with the **Ethical Guidelines for Trustworthy AI** (Annex II, Regulation (EU) 2024/1689).

4. Governance and Compliance Framework

4.1 EU AI Office and National Authorities

The governance structure established by the **EU AI Act** includes the creation of the **EU AI Office** and an **AI Board** composed of representatives from national authorities. These bodies are tasked with ensuring the effective enforcement of the regulation across the EU Member States (Article 63). The **EU AI Office** will provide guidance on compliance, while national authorities will have responsibility for enforcement within their jurisdictions (Article 63).

4.2 Legal Compliance and Monitoring

Under **Article 61**, providers of AI systems are required to conduct **post-market monitoring** to ensure continued compliance with the regulation after deployment. This includes reporting any incidents or malfunctions related to AI systems. The **AI Board** will oversee these processes to ensure consistent application of the Act’s provisions across Member States.

5. Sanctions for Non-Compliance

Non-compliance with the **EU AI Act** can lead to severe penalties, as outlined in **Article 63**. The maximum fine for violations can reach up to **EUR 35 million** or **7% of global annual turnover**, whichever is higher. This robust penalty regime underscores the importance of compliance with the regulation, particularly for high-risk AI systems.

6. Critical Reception and Future Challenges

The **EU AI Act** has been praised as a pioneering legal framework but has faced criticism, particularly regarding its complex **risk categorization system**. Some stakeholders argue that the definition of "high-risk" is too broad, and others have expressed concerns about the **costs** of compliance, especially for **SMEs** (Recital 37, Regulation (EU) 2024/1689).

The **European Data Protection Board (EDPB)** and other stakeholders have called for greater clarity in enforcement to avoid discrepancies between Member States (Article 58, Regulation (EU) 2024/1689).

7. Application of the EU AI Act in France

In **France**, the **Commission Nationale de l'Informatique et des Libertés (CNIL)** will play a pivotal role in the enforcement of the **EU AI Act**, particularly in the areas of **data protection** and **AI in public services**. France's established regulatory framework and AI strategy position it as a leader in **ethical AI** development within the EU (CNIL Guidelines, 2024).

8. Legal Implications of AI Use in Franchise Networks

The adoption of AI technologies within franchise networks in the EU presents a range of legal challenges and opportunities. The **EU AI Act** directly impacts franchise businesses that leverage AI systems in their operations, particularly with respect to **data privacy**, **transparency**, **accountability**, and **liability**.

Franchise networks often use AI systems for various purposes such as customer service (e.g., chatbots), data analytics, automated decision-making (e.g., loan approval, employee scheduling), and marketing strategies (e.g., personalized recommendations). As a result, both **franchisors** and **franchisees** must navigate the legal framework established by the **EU AI Act** to ensure compliance and mitigate legal risks.

8.1 Data Privacy and Protection

Franchise networks must be vigilant about the data they process through AI systems, especially with regards to customer and employee data. The **General Data Protection Regulation (GDPR)** provides a foundational framework for data protection, and it complements the **EU AI Act** in regulating how personal data is used in AI-driven applications. AI systems often rely on vast amounts of personal data, which increases the risk of violating **data privacy rights** (Article 5, GDPR).

For example, if a franchise network uses an AI system for personalized customer recommendations, it must ensure that the data used is collected with the explicit consent of the individuals concerned, as required under **Article 6** of the GDPR. Moreover, franchisees that implement such AI systems are also legally accountable for their compliance with data protection principles, including **data minimization** and **purpose limitation** (Article 5, GDPR). The **EU AI Act** adds a layer of accountability by enforcing the transparency of AI systems, meaning customers should be aware that AI is making decisions on their behalf (Article 11, Regulation (EU) 2024/1689).

8.2 Liability and Accountability

AI systems, particularly those involved in automated decision-making, raise questions about liability in the event of harm or error. Under the **EU AI Act**, responsibility for the operation and consequences of AI systems is attributed to both the **AI system provider** (typically the franchisor) and the **user** (usually the franchisee). This dual responsibility means that franchisees must ensure they are properly informed about the AI systems they use, including the risks and potential errors these systems might cause (Article 6, Regulation (EU) 2024/1689).

Franchisors, who develop or supply AI technologies to franchisees, must ensure that their AI systems are fully compliant with the **EU AI Act's** risk management and testing obligations, particularly for **high-risk AI systems**. If an AI system leads to harm or violates customers' rights, franchise networks must understand who is legally responsible and how to address claims effectively. The **EU AI Act** imposes **post-market monitoring** obligations, requiring businesses to report any incidents or system failures that could impact users' rights and safety (Article 61, Regulation (EU) 2024/1689).

Franchisees may face liability for non-compliance with the regulation if they fail to ensure that AI systems are properly monitored, tested, and used in accordance with the regulations. This includes ensuring that the AI systems respect privacy, do not cause unjust discrimination, and provide adequate explanations for their decisions when necessary (Article 13, Regulation (EU) 2024/1689).

8.3 Transparency and Consumer Protection

The **EU AI Act** emphasizes the need for transparency in AI systems, which is especially critical for franchise businesses that engage directly with consumers. Transparency requirements include informing customers when they are interacting with AI, ensuring that decisions made by AI systems are explainable, and providing customers with the ability to challenge decisions (Article 11, Regulation (EU) 2024/1689). For example, if an AI system used in a franchise network makes a decision about a customer's creditworthiness, the customer has the right to be informed about the factors influencing that decision and to challenge it.

Franchisees using AI-powered systems must be prepared to disclose how AI operates within their business processes, particularly when it impacts consumers' access to goods or services. Failure to meet transparency requirements could lead to reputational damage and potential legal consequences under both the **EU AI Act** and **consumer protection laws** (Directive 2005/29/EC).

Additionally, franchisors may need to help franchisees implement training and oversight mechanisms to ensure that AI systems used in customer-facing operations are fully transparent and aligned with consumer rights. For example, AI-driven pricing algorithms must not engage in discriminatory pricing practices based on factors like race, gender, or age. This is in line with the **EU Charter of Fundamental Rights**, which prohibits discrimination (Article 21, EU Charter).

8.4 High-Risk AI Systems and Compliance

Franchise networks must carefully evaluate whether the AI systems they use fall under the **high-risk** category defined by the **EU AI Act** (Article 6, Annex III). High-risk AI systems include those used for critical services, such as **healthcare**, **transportation**, **financial services**, and **employment decisions**. AI systems used in recruitment, for example, may be classified as high-risk if they involve significant decision-making impacts on employees' careers or financial stability.

If a franchise network uses a high-risk AI system, it must comply with more stringent requirements, including providing robust documentation, conducting risk assessments, and ensuring human oversight of AI decisions (Article 9, Regulation (EU) 2024/1689). This creates a significant legal burden on franchisees who operate in sectors like healthcare or finance, where the stakes are particularly high.

Franchisors providing high-risk AI technologies to their franchisees will need to ensure that these systems are fully compliant with the **EU AI Act's** testing, validation, and certification processes. For instance, AI systems used for employee monitoring must undergo thorough assessments to mitigate the risk of discrimination, in line with **EU employment laws** (Directive 2000/78/EC).

8.5 Cross-Border Implications

Since franchise networks often operate across multiple EU Member States, they must be mindful of the potential **cross-border implications** of the **EU AI Act**. The regulation applies uniformly across the EU, but national authorities may have different enforcement practices or interpretations of the Act. This necessitates a coordinated approach to ensure compliance across all jurisdictions where the franchise network operates.

Franchisors should provide clear guidelines and support to franchisees in navigating the legal complexities of AI compliance in various Member States. This includes addressing differences in national data protection rules, sector-specific regulations, and local interpretations of the **EU AI Act**. Additionally, franchise networks operating outside the EU may also face compliance challenges, as the **EU AI Act** applies to **third-country operators** offering AI systems or services to EU customers (Article 3, Regulation (EU) 2024/1689).

By considering these legal implications, franchise networks can mitigate the risks associated with AI deployment while complying with the **EU AI Act** and protecting both their customers and their businesses. The **EU AI Act** offers an opportunity for franchises to build trust with consumers and partners by demonstrating their commitment to ethical, transparent, and accountable AI usage.

9. Conclusion

The **EU AI Act** represents a groundbreaking shift in AI regulation within the European Union. By adopting a **risk-based approach**, the Act strikes a balance between encouraging technological innovation and safeguarding fundamental rights. For businesses, including franchise networks, this regulation presents both challenges and opportunities, particularly in navigating compliance requirements for **high-risk AI systems**. As the EU continues to lead the global regulatory agenda on AI, staying abreast of legal developments will be essential for businesses and legal professionals alike.

Legal Citations:

- Regulation (EU) 2024/1689, **Artificial Intelligence Act**, Official Journal of the European Union, 12 July 2024.
- **EU Charter of Fundamental Rights**, Official Journal of the European Union, 2012.
- **General Data Protection Regulation (GDPR)**, Regulation (EU) 2016/679, Official Journal of the European Union, 27 April 2016.
- **Commission Nationale de l'Informatique et des Libertés (CNIL)**, AI Guidelines (2024).