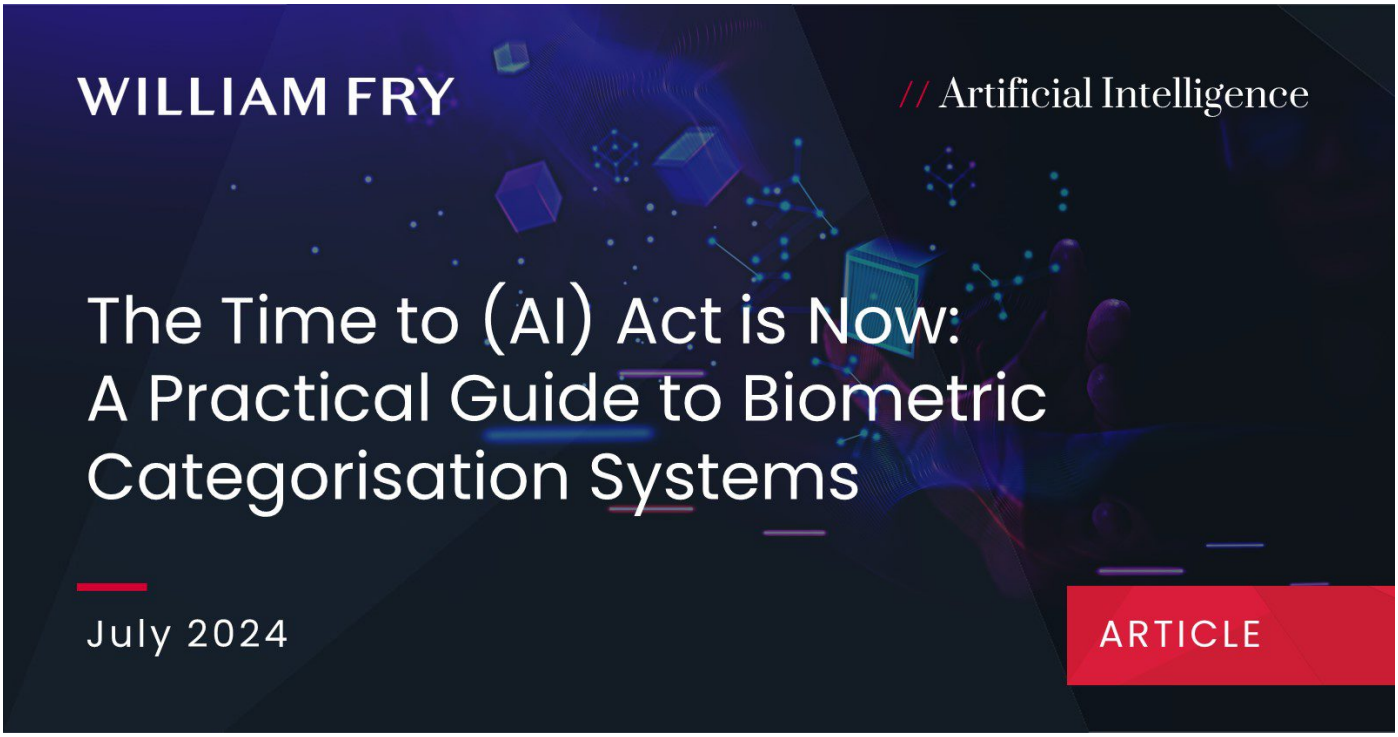
The Time to (AI) Act is Now: A Practical Guide to Biometric Categorisation Systems Under The AI Act

July 18, 2024



The AI Act's treatment of biometric categorisation systems is nuanced, particularly when distinguishing between prohibited and high-risk applications.

Article 3(40) defines a biometric categorisation system as one that assigns individuals to specific categories based on biometric data, unless it is ancillary to another commercial service and necessary for technical reasons. This distinction is crucial in understanding the broader regulatory landscape.

A. Overview of Biometric Categorisation Systems under the AI Act

Biometric data, as defined in Article 3(34), includes personal data resulting from processing related to physical, physiological, or behavioural characteristics. Article 3(35) extends this to biometric identification, involving the automated recognition of these characteristics to establish identity. The AI Act, therefore, places significant emphasis on the sensitivity and potential misuse of such data.

Article 5(g) prohibits the placing on the market, putting into service, or use of biometric categorisation systems that deduce or infer sensitive attributes such as race, political opinions, or sexual orientation. This prohibition is specific and absolute, aiming to prevent systems from making inferences that could lead to discrimination or privacy violations.

Recital 30 supports this by highlighting that while categorising datasets lawfully acquired for attributes like hair colour or eye colour may be permissible in law enforcement, deducing sensitive personal attributes is strictly prohibited.

In contrast, high-risk biometric categorisation systems, as referenced in Article 6(2) and detailed in Annex III, are subject to stringent regulation rather than outright prohibition. These systems, used for purposes like identifying sensitive or protected attributes, are considered high-risk due to the potential for significant harm or influence on decision-making outcomes. Recital 54 underscores the high-risk classification by noting the discriminatory potential and technical inaccuracies that could affect protected characteristics like age, ethnicity, or race.

Deployers of high-risk biometric categorisation systems must adhere to specific obligations under Article 50(3), including the obligation to inform individuals exposed to these systems and to process data in compliance with GDPR and other relevant EU regulations. This reflects the Act's intent to ensure transparency and safeguard individual rights, even for high-risk systems.

The key difference lies in the nature and sensitivity of the categorisation. Prohibited systems deduce or infer sensitive attributes from biometric data, while high-risk systems involve categorising biometric data in ways that could indirectly affect individuals' rights and outcomes.

The difference seems to be that biometric categorisation will be considered high-risk if sensitive attributes are readily apparent, but it will be prohibited if such attributes are inferred or deduced from other data.

Prohibited systems are outright banned due to their inherent risk of severe misuse and discrimination. In contrast, high-risk systems are regulated to ensure that they are used responsibly and with necessary safeguards to protect individual rights.

This distinction can lead to confusion, particularly where the line between sensitive inferences and lawful categorisations is blurred. For instance, while a system categorising images by hair or eye colour for law enforcement purposes might be high-risk and regulated, a system inferring someone's political beliefs from facial recognition data is prohibited. Navigating these nuances requires careful legal interpretation and compliance with both the AI Act and relevant national laws, ensuring that biometric technologies are deployed ethically and legally.

Furthermore, the overlap between national laws and the AI Act's provisions adds another layer of complexity. For example, Ireland's specific opt-outs under Recital 40 indicate that certain uses of biometric categorisation in law enforcement may be permissible under national law, despite the broader EU prohibition. This necessitates a detailed understanding of both Union and Member State regulations to navigate compliance effectively.

The regulatory framework's reliance on the context and purpose of biometric categorisation systems means that stakeholders must be vigilant in distinguishing between acceptable high-risk applications and outright prohibited practices. This vigilance is crucial to avoid unintentional breaches of the AI Act, given the severe implications of using these technologies improperly.

B. Key Dates:

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

1 August 2024: The AI Act will become law.

2 February 2025: Article 5 Biometric Categorisation Systems are banned.

2 August 2026: Rules on Annex III Biometric Categorisation Systems come into effect.

C. Enforcement and Penalties

Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35,000,000 or, if an undertaking, 7% of the offender's total worldwide annual turnover, whichever is higher. Non-compliant AI systems can also be taken off the EU market.

The AI Act imposes significant fines for non-compliance with its provisions, especially for high-risk AI systems. Non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).

Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7,500,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

For small and medium-sized enterprises (SMEs), including start-ups, each fine is capped at the lower of the specified percentages or amounts.

D. Steps to Compliance

1. Understand and Categorise Your Biometric System

Identify the Type of System:

- Determine if your system is a biometric categorisation system or a biometric identification system.
- Assess whether your system deduces sensitive attributes (e.g. race, political opinions, sexual orientation) or if it categorises non-sensitive attributes (e.g. hair colour, eye colour).

2. Assess the Legal Requirements

Prohibited Systems (Article 5(g)):

- Verify if your system deduces or infers sensitive attributes.
- Ensure that such systems are not placed on the market, put into service, or used.

High-Risk Systems (Article 6(2) and Annex III):

- Identify if your system falls under high-risk categories as defined in Annex III.
- Understand the regulatory requirements for high-risk systems.

3. Implement Necessary Safeguards for High-Risk Systems

Compliance with GDPR and EU Regulations:

- Ensure all data processing complies with GDPR and relevant EU regulations.
- Implement robust data protection measures.

Transparency and Notification:

- Inform individuals exposed to high-risk biometric categorisation systems.
- Provide clear information on data processing purposes and their rights.

4. Conduct a Risk Assessment and Mitigation Plan

Risk Analysis:

- Perform a thorough risk assessment to identify potential harms and discriminatory impacts.

Mitigation Strategies:

- Develop and implement strategies to mitigate identified risks.
- Regularly review and update mitigation measures.

5. Documentation and Record-Keeping

Maintain Records:

- Keep detailed records of compliance measures, risk assessments, and mitigation plans.
- Document the decision-making process and any consultations with legal or technical experts.

6. Regular Monitoring and Audits

Continuous Monitoring:

- Regularly monitor the operation of high-risk systems for compliance.
- Implement a mechanism for ongoing review and improvement.

Independent Audits:

- Conduct independent audits to ensure compliance with the AI Act and related regulations.

7. Training and Awareness

Employee Training:

- Train employees on compliance requirements, data protection, and ethical use of biometric systems.
- Ensure all staff understand the importance of adhering to legal and regulatory standards.

8. Stay Informed on Legal Developments

Legal Updates:

- Keep abreast of changes and updates in the AI Act and relevant national laws.

Adjust compliance strategies accordingly to ensure ongoing adherence to new regulations.

In summary, while the AI Act provides a structured approach to regulating biometric categorisation systems, the fine line between prohibited and high-risk applications demands thorough understanding and careful application of the law. The potential for confusion underscores the need for clear guidance and robust compliance mechanisms to ensure that the deployment of such technologies aligns with both legal requirements and ethical standards.

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.

Contributed by Thomas Martin.