PUBLICATION

Analyzing the EU Artificial Intelligence Act: Spotlight on Biometrics

Authors: David J. Oberly
May 16, 2024

The European Parliament formally adopted the EU Artificial Intelligence Act (AI Act), a first-of-its-kind comprehensive regulation governing the use of artificial intelligence (AI), on March 13, 2024. While applicable to a wide range of AI, the AI Act places a significant focus, in particular, on regulating biometric technologies that rely heavily on advanced algorithms and models.

The AI Act places stringent, detailed requirements on the vast majority of biometric systems in operation today, even going so far as to ban certain use cases altogether. The AI Act also has an expansive extraterritorial reach that subjects a wide range of companies with no operations or physical presence in the EU to comply with the new regulation.

Combined, companies that develop, supply, or use biometrics today (or intend to do so in the near future) are advised to take proactive steps to determine whether they are subject to compliance with the AI Act and, if so, formulate a concrete action plan to achieve compliance in advance of the time the AI Act goes into effect.

Key Aspects of the AI Act Implicating Biometrics

Scope of Regulated Technologies and Systems

The AI Act directly regulates a wide range of biometric technologies, including those that perform the following functions:

- **Biometric Identification.** Automated recognition of physical, physiological, behavioral, or psychological human features for the purpose of establishing a person's identity by comparing that person's biometric data to the biometric data of persons stored in a reference database.
- **Biometric Verification.** Automated, one-to-one verification, including authentication, to confirm that a specific person is who he or she claims to be.
- **Biometric Categorization.** Assignment of persons to specific categories – such as sex, age, behavioral or personality traits, sexual orientation, or political orientation – based on their biometric data.

The EU regulation also singles out several specific types of biometric technologies, subjecting them to the highest level of requirements and restrictions imposed by the AI Act and, under certain circumstances, going even further to impose a blanket prohibition over their use:

- **Emotion Recognition Systems.** An AI system used for the purpose of identifying or inferring emotions or intentions – such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, concept, satisfaction, and amusement – of persons based on their biometric data;
- **Biometric Categorization Systems.** An AI system that processes biometric data, such as a face or fingerprint, to assign persons to specific categories, such as sex, age, hair color, eye color, tattoos, behavioral or personality traits, language, religion, sexual orientation, or political orientation;

- **Remote Biometric Identification Systems.** An AI system intended for use in identifying persons, without their active involvement and typically at a distance, through the comparison of their biometric data with biometric data contained in a reference database;
- **Real-Time Remote Biometric Identification Systems.** A type of remote biometric identification system where the capture and comparison of biometric data, and the resulting identification of persons, all occur without significant delay to avoid circumvention; and
- **Post-Remote Biometric Identification Systems.** A type of remote biometric identification system that uses previously captured biometric data to complete the comparison and identification process only after a significant delay.

Compliance Throughout the Biometrics/AI Value Chain

One of the most notable aspects of the AI Act is its allocation of compliance obligations across relevant actors throughout the AI value chain, according to their respective roles. As discussed in more detail in our prior EU AI Act Client Alert, Who's Who Under the EU AI Act: Spotlight on Key Actors, the AI Act applies to the following, referred to collectively as "operators" under the AI Act:

- **Providers**. An entity that develops AI systems or general-purpose AI (GPAI) models (discussed in more detail below) and places them on the EU market or puts them into service under their own name or trademark;
- **Deployers**. An entity that uses AI systems under its own authority;
- **Product Manufacturers**. An entity that provides, distributes, or uses AI systems in the EU together with its products under its own name or trademark;
- **Distributors**. An entity in the supply chain, other than a provider or importer, that makes an AI system available on the EU market; and
- **Importers**. An entity located or established in the EU that places an AI system on the market bearing the name or trademark of another entity established outside of the EU.

Extraterritorial Reach

As indicated above, the AI Act has expansive territorial reach, extending to all companies – even those without any physical presence or operations in the EU – that:

- provide (*i.e.*, develop, supply, manufacture, etc.) or market/offer biometric systems for use in the EU; or
- provide or deploy (*i.e.*, use) biometric systems that generate outputs that are used in the EU.

The broad exterritorial applicability of the AI Act will require a wide range of companies to adapt to the EU's new, comprehensive regulatory scheme, regardless of the location of their core operations or primary market focus.

Administrative Fine Scheme

The AI Act imposes steep administrative fines for non-compliance, which entail the following:

- **Prohibited AI Violations.** Up to 35 million euros or seven percent of worldwide annual turnover (whichever is greater);
- **Most Other Violations.** Up to 15 million euros or three percent of worldwide annual turnover (whichever is greater); and
- **Incorrect, Incomplete, or Misleading Information Supplied to Authorities.** Up to 7.5 million euros or one percent of worldwide annual turnover (whichever is greater).

Timeline for Enactment

The bulk of the AI Act, including the majority of obligations for high-risk systems, will go into effect two years after publication in the Official Journal of the European Union, *i.e.*, sometime in mid-2026. Certain elements, however, will take effect before or after the two-year mark:

- the prohibition on unacceptable risk AI practices will become applicable after six months;
- the majority of obligations pertaining to GPAI model governance will become applicable after 12 months; and
- obligations relating to high-risk product components covered by EU harmonization legislation, and GPAI models on the market as of the effective date of the AI Act, will become applicable after 36 months.

AI Act's Risk-Based Regulatory Approach & Implications for Biometrics

The AI Act utilizes a risk-based regulatory framework, imposing different obligations based on three primary risk levels: (1) unacceptable risk; (2) high risk; and (3) transparency risk. In addition, also included is a fourth classification pertaining to GPAI models, which are defined as AI models that display significant generality and are capable of performing a wide range of distinct tasks, and which can be integrated into a variety of downstream systems or applications.

Unacceptable Risk

The unacceptable risk classification entails AI systems and practices that present a threat to privacy, data protection, non-discrimination, and other fundamental rights. The AI Act imposes a blanket prohibition over all systems and practices that fall under this category, which includes the following biometric technologies and use cases:

- the use of biometric categorization systems to make *inferences* – such as those relating to political opinions, trade union membership, religious or philosophical beliefs, race, sex life, or sexual orientation – based on persons' biometric data;
- the use of emotion recognition systems in employment and education settings;
- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; and
- real-time remote biometric identification systems used in publicly accessible spaces for law enforcement purposes.

High-Risk

The high-risk classification entails AI systems that pose a significant risk of harm to fundamental rights, safety, or health, but which can be addressed and mitigated through the implementation of appropriate safeguards.

The following biometric use cases fall under the high-risk category:

- remote biometric identification systems that are *not* used solely to provide access to a service, unlock a device, or gain secure access to a restricted premises;
- biometric categorization systems that use biometric data to categorize individuals according to their sensitive attributes or characteristics; and
- emotion recognition systems (which are not otherwise prohibited under the AI Act).

High-risk systems are subject to strict compliance obligations both before and after the time they are put on the market, including the following:

- risk management systems;
- data governance systems;
- quality management systems;
- fundamental rights impact assessments;
- conformity assessments;
- detailed technical documentation;
- transparency standards and use instructions;
- accuracy, robustness, and security standards;
- cybersecurity resilience;
- automatic event recording (logging) capabilities; and
- human oversight.

Transparency Risk

The transparency risk classification entails systems that present risks relating to misinformation and manipulation at scale, fraud, impersonation, and consumer deception. Notably, these transparency obligations are applicable under certain circumstances to systems that are also subject to the AI Act's high-risk obligations.

The following biometric systems fall under this classification, each of which is subject to a separate, distinct set of obligations:

- **Emotion Recognition Systems and Biometric Categorization Systems.** Must bear visible information providing notice to data subjects; also, must process personal data in accordance with applicable GDPR obligations;
- **Deepfake Systems.** Must disclose that the output content produced by the system has been artificially generated or manipulated with the use of AI; and
- **AI Systems and GPAI Models That Generate Synthetic Content.** Must mark system outputs in a machine-readable format and in a manner that makes such outputs detectable as artificially generated or manipulated with the use of AI.

GPAI Models

GPAI models are subject to their own set of compliance obligations – applicable regardless of risk level – which entails the following:

- training, testing, and evaluation of technical model documentation;
- GPAI model capability/limitation documentation for AI system providers;
- internal policies for complying with EU copyright law;
- GPAI model training data disclosures made available to the public; and
- authorized representative appointment (for providers established outside of the EU).

In addition, the AI Act imposes heightened obligations on GPAI models that are deemed to present "systemic risk," which under the AI Act means risks specific to the most advanced GPAI models that have a significant impact on the EU market due to their reach or their potential to produce negative effects on the public as a whole, and which can be propagated at scale across the value chain.

GPAI models with systemic risk must satisfy: (1) the obligations imposed on all GPAI models; and (2) the following additional obligations:

- model evaluations, including adversarial testing to identify and mitigate risk;
- assessment and mitigation of potential EU-level systemic risks;

- cybersecurity protections; and
- reporting and remediation of incidents or AI system malfunctions causing serious injury or harm.

Practical Compliance Tips and Strategies

What to Do Now

Companies that develop, supply, or operate biometric systems should begin the process of working toward compliance with the AI Act now to allow for sufficient time to complete all modifications and enhancements to current organizational compliance programs needed to achieve compliance in advance of the regulation's phased implementation timeline.

Companies can consider the following high-level action plan for adapting current practices for compliance with the AI Act. In addition, following the action steps outlined below will provide the added benefit of helping to prepare for similar laws and regulations that may soon follow on the heels of the EU's groundbreaking AI regulatory scheme.

1. **Complete a Biometric System Inventory.** Identify and document all biometric systems and models that your organization currently develops, deploys, or otherwise has in operation at this time.

2. **Evaluate AI Act Applicability.** For each identified system, conduct a threshold applicability and impact analysis to determine whether the system is subject to compliance with the AI Act and, if so, how operations and other aspects of your organization may be impacted. For U.S. companies, careful consideration should be given to whether the AI Act applies extraterritorially to your biometric systems.

3. **Determine Applicable Risk Classification and Role in AI Value Chain.** For each system determined to be within scope, determine the appropriate risk classification (*i.e.*, unacceptable, high, transparency, and/or GPAI model) and your organization's role in the AI value chain (*i.e.*, provider, deployer, manufacturer, importer, or distributor).

4. **Conduct a Compliance Gap Analysis.** For each in-scope system, evaluate the level of alignment between your organization's current compliance practices and the specific obligations imposed under the AI Act to identify any gaps that will need to be remediated to achieve compliance.

5. **Develop a Compliance Roadmap.** Based on the results of the gap analysis, formulate a concrete action plan for executing all modifications and enhancements to organizational compliance programs necessary to address identified compliance gaps ahead of the AI Act's phased enactment timeline.

Involve Experienced Outside Biometrics and AI Counsel Early in the Process

The AI Act will require companies that operate in the biometrics sector (and beyond) to adapt their business practices and processes to align with the new rules and standards set forth in the EU regulation. Companies should expect to expend substantial time and resources – and to incur significant costs – in executing necessary modifications and enhancements to current compliance programs to come into compliance with the AI Act.

To manage and limit these costs, companies should seek to involve experienced outside biometrics and AI counsel early in the process. For existing biometrics systems, outside counsel can provide key guidance and insight to streamline the compliance program evaluation and modification process. And for new biometric systems, counsel can assist in bringing legal compliance issues to the forefront so they are adequately

considered and addressed during all phases of the development/acquisition process and up through the time of system rollout or launch (and, ideally, thereafter throughout the duration of the system lifecycle).

Baker Donelson's Biometrics and Artificial Intelligence Teams Can Help

Baker Donelson's Biometrics and Artificial Intelligence attorneys regularly counsel clients on the use of biometrics and related AI systems and tools in their businesses, and provide guidance on the current and anticipated legal and regulatory landscape that must be addressed when using these advanced technologies. At the same time, our Biometrics and Artificial Intelligence teams closely monitor for new biometrics and AI legislative and regulatory developments worldwide, as well as emerging trends applicable to the biometrics and AI sectors.

For more information or assistance with EU AI Act compliance, or any related biometrics or AI matters, please contact David Oberly or another member of Baker Donelson's Biometrics, Artificial Intelligence, or Data Protection, Privacy, and Cybersecurity Teams.