Articles + Publications | May 3, 2022

The EU Is Throwing Stones in the Data Lake by Regulating AI – What Global Companies Need to Do Now to Prepare

WRITTEN BY

Robert A. Angle | James Koenig | Gerar Mazarakis

This article was originally published on May 3, 2022 in IPWatchdog. It is republished here with permission.

High-stakes artificial intelligence (AI) is becoming even higher risk in the European Union, where AI regulation efforts are underway that could cost your company up to 6% of its total worldwide revenues—more than the potential penalties for privacy violations under the EU's General Data Protection Regulation (GDPR). On April 21, 2021, the European Commission proposed rules for regulating AI (the AI Act or Act), to which the European Parliament recently released proposed amendments on April 20, 2022. The Act may undergo a series of additional amendments, but a final text is nearing completion and European countries are starting to act in anticipation of the regulation. Companies should plan for the comprehensive act to become law and begin implementing best practices now to ensure a competitive advantage. Below is an overview of the AI Act's key provisions that takes into account the Parliament's recent changes.

The Act will apply to entities placing on the market or putting into service AI systems in the Union regardless of whether the entity is in the Union or in a third country, entities in the Union using AI systems, and entities using AI systems in a third country when the output of the system is used in the EU or affects persons in the Union. The Act follows a risk-based approach **prohibiting unacceptable systems**, creating requirements for **high-risk systems**, and establishing transparency obligations for certain systems, including **non-high-risk systems**, explained below.

While the Act recognizes that AI has many beneficial uses, it also recognizes that technology can be misused and provide new, powerful tools for malevolent practices contradicting Union values of respect for human dignity, freedom, equality, democracy, and the rule of law, in addition to Union fundamental rights such as non-discrimination, data protection and privacy, and children's rights. Consequently, the Act generally prohibits AI systems that are used for practices including the following:

- Individual risk assessment for predictive policing;
- Using subliminal techniques such as sounds, images, and text to subconsciously alter a person's behavior;

- Exploiting vulnerabilities due to age or physical or mental disability to alter a person's behavior;
- Social scoring; and
- Real-time biometric identification for law enforcement, subject to exceptions such as antiterrorism.

Recognizing that high-risk AI systems should only be used or placed in the market if they meet certain mandatory requirements, the Act creates a list of high-risk AI systems posing a significant harmful impact on the health, safety, and fundamental rights of persons in the Union. High-risk systems include systems used for the following:

- Biometric identification;
- Management and operation of critical infrastructure;
- Education and vocational training;
- Employment;
- Essential private and public services;
- Law enforcement;
- Migration, asylum, and border control;
- Administration of justice and democratic processes; and
- Safety components of products, or products, covered by certain EU regulations.

The Act mandates that the list of high-risk AI systems will be regularly evaluated and imposes the following requirements for such systems:

- *Risk Management* – A risk management system must be established, implemented, documented, and maintained in relation to high-risk AI systems.
- *Data and Data Governance* – Training, validation, and testing data sets must meet certain quality criteria such as accuracy, privacy, bias prevention, minimization.
- *Technical Documentation* – Technical documentation must be drawn up before the AI system is placed on the market or put into service and must be kept up-to-date.

- *Record Keeping* – High-risk AI systems must enable automatic recording of event logs for monitoring the system's operation.

- *Transparency* – Systems must enable users to interpret the output and use it appropriately.

- *Human Oversight* – Systems must enable effective oversight by natural persons.

- *Accuracy, Robustness, and Cybersecurity* – Systems must achieve, in light of their intended purpose, an appropriate level of accuracy, robustness, and cybersecurity.

Additionally, providers of high-risk AI systems, including third parties placing the system on the market under their name or trademark or making a substantial modification to the system, are responsible for ensuring compliance with the Act, including having a quality management system in place, drawing up technical documentation, maintaining logs when under their control, post-market monitoring, and reporting any serious incidents or malfunctions. Providers must also ensure the system undergoes a conformity assessment procedure and is registered in an EU database.

Depending on the type of system, the provider must either conduct an internal conformity assessment procedure, wherein the provider self-certifies the system's conformity with the Act, or have a separate body conduct the assessment and issue a certificate. Systems must undergo a new conformity assessment whenever they are substantially modified. For systems that continue to learn after being placed on the market or put into service, however, changes to the system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are included in the technical documentation will not constitute a substantial modification. Providers must draw up a written EU declaration of conformity for each AI system and keep it at the disposal of European authorities for 10 years after the system has been placed on the market or put into service.

The Act also grants European authorities access to datasets and, where necessary, source code to ensure compliance. Authorities can also require that corrective actions be performed to bring a system into compliance with the Act or that the system be removed from the market.

While non-high-risk AI systems are not subject to the same restrictions as high-risk AI systems, the Act imposes transparency obligations for certain systems. The Act's transparency obligations, which are intended to allow people to make informed choices or avoid interaction with AI systems, are the following:

- For systems intended to interact with people, providers must ensure that the system is designed and developed in such a way that the person is informed that she is interacting with AI unless this is obvious from the context.

- Users of an emotion recognition system or a biometric categorization system must inform persons exposed to the systems of the system's use.

- Users of “deepfake” AI systems (i.e., systems that generate false images, audio, or video of people, places, objects, or events in a way that would trick a person into believing the content is real) must disclose that the content has been artificially generated or manipulated. Note that deepfakes impersonating real persons and editorial content written by AI (AI authors) are subject to both transparency requirements and the conformity requirements of high-risk systems.

The Act’s only obligations for non-high-risk AI systems, such as chatbots, are the transparency obligations mentioned above. However, the Act explains that providers of non-high-risk AI systems should be encouraged to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk systems.

The AI Act will start being enforced 24 months after it is adopted by the EU and published in the Union’s Official Journal. According to Euractiv, on April 25, 2022, the French Presidency leading the Council’s work shared a new compromise text proposing several changes to the Act to be discussed with representatives of other member states at an April 27 telecom working party. Countries are starting to take action in anticipation of the act, and on April 5, 2022, France’s data protection agency, the Commission Nationale de l’informatique et des Libertés (CNIL), published guidance on AI discussing the importance of recognizing the presence of AI, reasons behind errors made by AI, and support the CNIL offers for developing AI systems. Similarly, on April 4, 2022, Germany’s Federal Commissioner for Data Protection and Freedom of Information (BfDI), published a report on AI in law enforcement and security calling for timely action by the legislature.

The AI Act includes data collection requirements such as bias prevention and privacy in its regulations for high-risk systems, and companies in Europe are starting to comply with these provisions to varying degrees. Further, these principles reflect globally-emerging ethical guidelines for AI that companies around the world are taking note of and as a result, are starting to adopt the following best practices on a broad scale in order to have homogenous and interoperable data to maintain a competitive advantage:

- **conducting ethics assessments** to identify discriminatory impacts and privacy implications such as identifiability;

- **establishing AI internal ethical charters** outlining ethical data collection and use requirements and procedures, and

- **developing contractual requirements and minimum data handling and security controls for vendors and third parties** with whom data is shared to pass along such ethical requirements and use restrictions (e.g., prevent discrimination, targeted advertising, location tracking restrictions).

Businesses should start implementing these practices as soon as possible to avoid lagging behind the competition

and to avoid having to delete data in their data lake, restart data collection, or retrain algorithms if data collection and use is not done in accordance with these global ethical considerations and the final requirements of the AI Act.

RELATED INDUSTRIES + PRACTICES

- Technology
- Artificial Intelligence
- Privacy + Cyber
- Data + Privacy