The coming era of AI regulation

Taking Notice of AI Regulation

On April 21, 2021, the European Commission unveiled the Artificial Intelligence Act (EU AI Act). It is supported by the EU Commission and is expected to be ratified by the EU Parliament.

It will introduce a sophisticated "product safety framework" composed of four risk categories. It imposes requirements for the market entrance and certification of high-risk AI Systems through a mandatory CE-marking procedure. This pre-market conformity regime also applies to the training, testing, and validation datasets of machine learning programs.

In short, as far as data governance is concerned, following requirements must be satisfied:

> *High-risk AI systems must be developed using **quality datasets**, including those used for training, validating and testing the algorithm. Concretely, this quality requirement means **that data must be relevant, representative, free of errors and complete.** In addition, good data management practices such as **paying particular attention to biases as well as to data gaps and data shortcomings are also mandatory.**[1]*

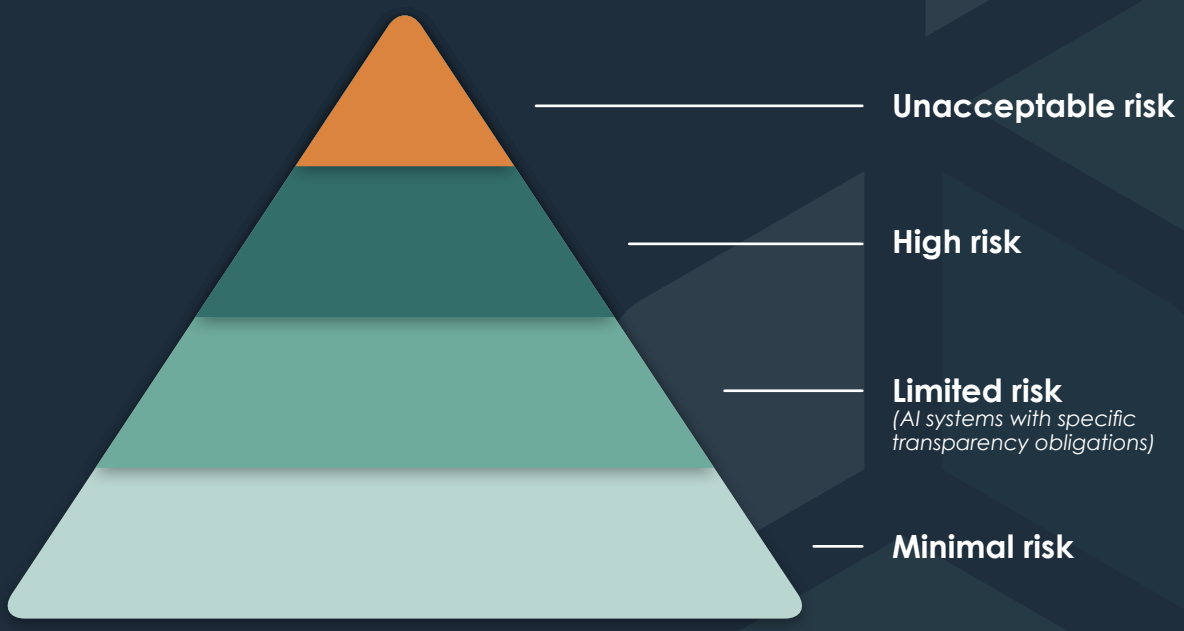
The EU AI Act not only regulates sophisticated deep learning and natural language processing systems but also covers a very broad range of techniques that are not commonly referred to as "AI." These include statistical methods, search, and inference. If you are processing data, it is likely your current methods are covered by the Act.

[1] *Eve Gaumond, "Artificial Intelligence Act: What Is the European Approach for AI?" Lawfare, June 4, 2021, https://* ***www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai***

Modulos AG, Technoparkstr. 1, 8005 Zurich, Switzerland UID: CHE-233.391.866 | **contact@modulos.ai** | **+41 76 566 05 48**

Figure 1

The Pyramid of Criticality for AI Systems



Source: Mauritz Kop, "EU Artificial Intelligence Act: The European Approach to AI," Stanford-Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University 2(2021).

High-risk AI systems must be carefully assessed before reaching the market. And throughout their life cycle, they will have to be continuously audited and tracked.

Many products and services—currently either unregulated or lightly regulated—may be placed in the high-risk category. This will require companies to reevaluate and possibly rebuild their AI systems.

Some examples include:

- Critical infrastructure that could put the life and health of citizens at risk (e.g., transport).
- Educational or vocational training that may determine someone's access to education or professional advancement (e.g., scoring of exams).
- The safety components of products (e.g., AI applications used in robot-assisted surgery).
- Employment, human resources, and access to self-employment (e.g., resume-sorting software for recruitment procedures).
- Essential private and public services (e.g., credit scoring that denies loan approval).
- Law enforcement that may interfere with fundamental rights (e.g., evaluation of evidence).
- Migration, asylum, and border control management (e.g., verification of travel documents).
- Administration of justice and democratic processes (e.g., applying laws to a concrete set of facts).
- Surveillance systems (e.g., biometric monitoring, facial recognition systems).

Modulos AG, Technoparkstr. 1, 8005 Zurich, Switzerland UID: CHE-233.391.866 | **contact@modulos.ai** | **+41 76 566 05 48**

A pre-market conformity mechanism is defined in the Act. It will work similarly to the mechanism required for CE marking (which certifies the safety of products sold in the European market).

Given this wide range of regulatory areas of interest, it is incumbent on companies to find efficient, cost-effective, and exhaustive tools to ensure compliance.

How will Modulos help you do this?

Our Data Quality Management (DQM) system assists human data scientists in their mission to deliver quality data for machine learning projects.

It can help identify crucial missing data, potential outliers, noisy items, and whether data is fair with respect to its subgroups.

Modulos DQM provides transparency for users. Those developing high-risk AI systems ("providers" under the proposed regulation) must disclose certain types of information to ensure proper use of such systems. For example, providers must disclose information about the characteristics, capabilities, and limitations of the AI system, along with the system's intended purpose and information necessary for its maintenance and care. Producing such disclosures is an automated aspect of the Modulus system.

How Does Modulos Do All of This?

All ML models trained using Modulos AutoML are open and ready for analysis and inspection.

Each trained model comes with precomputed insights that characterize the model. This facilitates the meeting of any testing, documentation, or disclosure requirements.

Such oversight includes surveilling for automation bias problems, spotting anomalies or signs of dysfunctions, deciding whether to override an AI system's decision-making, or pulling the "kill switch" if a system poses a threat to the safety or fundamental rights of people.

modulos

Get a demo today at **modulos.ai/get-started/**

Modulos Data-Centric AI platform revolutionizes the way safe and trustworthy AI applications are built. System-guided recommendations assist business leaders in their AI journey to create reliable ML models in their own domain of expertise

Modulos AG, Technoparkstr. 1, 8005 Zurich, Switzerland UID: CHE-233.391.866 | **contact@modulos.ai** | **+41 76 566 05 48**

The AI Is Never In Complete Control

High-risk AI systems must be designed to operate with human oversight.

Importantly, this does not mean that individuals or teams must have a precise understanding of how AI systems—often described as black boxes—come to a particular decision. Instead, the focus is on the capacity to understand the main limitations of AI systems and the ability to identify such shortcomings in a particular system.

The data-centric approach that is at the core of the Modulos system enables humans to be in the loop during the initiation process and assists in addressing issues of poor data and bias. The open nature of models built by AutoML means that the latest techniques to explore and characterize ML models are easily applied so that no model remains a black box. Safe, Yet Powerful.

The Modulos platform helps data scientists and engineers build secure and robust AI systems. We provide the ability to "robustify" models automatically, making them less liable to noise. The platform is also designed with security in mind with strong backup and restore functionality. There is also the ability to run in secure on-premise environments. Internet access is only required during initial installation.

High-risk AI systems must achieve a level of accuracy, robustness, and cybersecurity that is proportionate to their intended purpose. Providers will be obligated to communicate accuracy metrics to clients. Backup or fail-safe plans that ensure sufficient robustness will also be required, as will technical solutions to prevent cybersecurity incidents (such as data poisoning).

"High-risk AI systems must achieve a level of accuracy, robustness, and cybersecurity that is proportionate to their intended purpose."

Providers must also establish technical documentation that contains the necessary information for assessing compliance with other requirements mentioned above, including traceability and auditability. The extensive list of things that must be documented—like data management practices and risk management systems—can be found in Annex IV of the EU AI Act. Moreover, automatic recording of events (logs) is mandatory under the proposal.

modulos

Get a demo today at **modulos.ai/get-started/**

Modulos Data-Centric AI platform revolutionizes the way safe and trustworthy AI applications are built. System-guided recommendations assist business leaders in their AI journey to create reliable ML models in their own domain of expertise

Modulos AG, Technoparkstr. 1, 8005 Zurich, Switzerland UID: CHE-233.391.866 | **contact@modulos.ai** | **+41 76 566 05 48**

Modulos Is a Comprehensive Solution That Provides Protection

Every step the Modulos platform takes—and every decision a human user makes—will be logged. This record will be available for audits in support of data management strategies and other reporting requirements.

Providers can comply with many requirements through a self-assessment procedure. Once the compliance assessment is done, the provider of an AI system completes an EU declaration of conformity, after which the CE marking can be ascribed and the European market entered. Fines for violating EU AI Act can be up to 6% of global turnover or €30 million for private entities.

The EU AI Act will set the de facto standard for AI regulation outside the EU, in the same way that the General Data Protection Regulation (EU GDPR) set the global standard for online privacy. Non-EU companies wishing to do business in Europe will have to comply, while other countries will introduce similar regulatory frameworks.

The Modulos DCAI platform is built to meet European AI regulations. Thanks to its novel data-centric AI approach, it provides all the tools necessary to address the regulatory intent inherent in the EU AI Act. ■

References

European Commission. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* European Union. April 4, 2021.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Gaumond, Eve. "Artificial Intelligence Act: What Is the European Approach for AI?" Lawfare, June 4, 2021.

https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai

Kop, Mauritz. "EU Artificial Intelligence Act: The European Approach to AI." *Stanford-Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University 2(2021).*

https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/

modulos

Get a demo today at **modulos.ai/get-started/**

Modulos Data-Centric AI platform revolutionizes the way safe and trustworthy AI applications are built. System-guided recommendations assist business leaders in their AI journey to create reliable ML models in their own domain of expertise

Modulos AG, Technoparkstr. 1, 8005 Zurich, Switzerland UID: CHE-233.391.866 | **contact@modulos.ai** | **+41 76 566 05 48**