Risk and Compliance in the Digital Age: Assessing the Impact of the European AI Act

Executive Summary

Many believe that artificial intelligence (AI) will be the "next big thing" in the digital era. Customers and businesses are increasingly using this technology to complete tasks that were previously limited to human operators and to solve problems. AI is a logical accelerator that can be applied to an almost limitless number of domains to perform the widest range of tasks. Since its penetration can affect any industry, its broad nature increases its potential impact on current economies. The case studies and suggested implementations capably demonstrate this. Artificial intelligence can be used to make better strategic choices, offer services or goods, enforce the law, streamline document drafting, and even produce art. Its widespread application might have an effect on daily tasks comparable to how manual labour was impacted by the industrial revolution.

Companies should begin assessing AI's effects on their business models in light of the features and potential that have been mentioned. This will allow them to take advantage of opportunities and reduce risks. Directors and compliance officers should avoid taking the potentially fatal risk of being caught off guard in any company. Likewise, directors should make sure that current regulations are followed if the growing use of AI-based solutions presents a pertinent opportunity for businesses, if not a requirement. Implementing AI solutions too quickly could have negative effects on reputation and regulations. In this regard, efficiency and compliance must be carefully weighed.

What’s cooking in the EU?

Co-legislators in the EU have been working on a comprehensive law, known as the AI Act, for the past two years. Given that a consensus on a definitive text is anticipated for the upcoming trilogue on December 6th, it appears that the Act is nearing its conclusion. Once approved, the Act will serve as a basic guidebook for any business in Europe wishing to use, introduce into the market, or put AI-based solutions into operation.

Even though the Commission's proposal is the text that is currently available, businesses should plan ahead to avoid being caught off guard by the final version. This is because a poorly conceived or executed compliance framework will make it impossible to distribute goods or provide services within the European Community.

The Keys of the AI Act. Scope, Definition, and Strategy

Firstly, the **scope**. Aside from certain exclusions, such as AI systems used for military purposes, the regulation covers any provider that: 1) installs or markets AI systems in the Union, regardless of whether the provider is based there or in a third country; 2) utilises AI systems installed within the Union; and 3) provides and uses AI systems located in a third country, where the system's output is used in the Union. As with other Union compliance regulations, such as the GDPR, the Act's scope is expressly broad. It is crucial to emphasise that any provider hoping to join the Union's market will need to comply, not just those based in the EU.

Secondly, the **definition of AI**. According to its definition, artificial intelligence (AI) is "software that is developed with one or more of the techniques and approaches listed in Annex I and can generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with, for a given set of human-defined objectives." This definition consists of two parts.

- Firstly, the techniques. **There are three possible techniques that** – following the proposal’s Annex – **can constitute AI**: 1) **Machine learning approaches**, including supervised, unsupervised and reinforcement learning, which use a wide variety of methods including deep learning; 2) **Logic and knowledge-based approaches**, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; 3) **Statistical approaches, Bayesian estimation, search and optimisation methods**.
- Secondly, the impact. **Regulated software is only those that can influence the surrounding environment, thus have an external impact**.

Lastly, the **regulatory approach**. At its core, the Act is fundamentally structured as a **product safety regulation**. It separates AI goods into three potential groups: 1) prohibited practices; 2) high-risk systems; 3) low or minimal risk systems. The classification is mainly based on the use of AI – such as the industry where the software is applied in or the purpose it serves – rather than rooted in the technology. The regulation requires a wide range of compliance obligations, such as transparency, safety, testing, etc., depending on the level of risk. This puts the Act firmly under the jurisdiction of "compliance regulations." This indicates that the Act mandates that businesses evaluate and reduce risks, but also do so in a methodical and structured way. For instance, Article 9 of the Act requires that “risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems”. Therefore, risk and compliance officers must make sure that a strong compliance framework is in place before AI software is used, developed, or marketed

AI ACT and GDPR: 2 parallel lines intended to cross each other

When designing, implementing or using AI, companies should also be mindful of their Data Protection duties. As clearly stated by the Act "the proposal is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679). In this way, the Act complements the GDPR rather than replacing it, requiring businesses to have a comprehensive grasp of their compliance obligations.

Then, in order to improve human control and transparency, AI should be developed, designed, and implemented in a trustworthy and responsible manner, based on the primary tenets of the General Data Protection Regulation 2016/679. Additionally, an AI tool used in the processing of personal data needs to be trained and used specifically for that purpose in order to comply with data privacy laws.

This specific goal should be determined in advance while considering the GDPR's Article 25 on privacy-by-design and privacy-by-default. It also involves figuring out how the processing will be done and putting in place the necessary organisational and technical safeguards to ensure that data protection laws are followed.

Six legal bases are listed in the GDPR, including consent, following the law, fulfilling a contract, completing a public interest mission, protecting vital interests, and pursuing a legitimate interest. However, a particular GDPR provision will affect AI-based choices about personal data and specific data categories (Article 9 of GDPR), as well as decisions about automated decision-making and profiling in accordance with Article 22 of GDPR. The GDPR contains a number of provisions that cover automated decision-making and profiling, as well as those related to access and objection rights.

AI ACT and Data Act: reuse of data and artificial intelligence constraints

The legality of primary data handling operations, such as access, reading, analysing, exporting, and training AI systems, is a major concern in the field of artificial intelligence (AI) data utilisation, especially when working with copyrighted materials. The lack of clear regulatory guidelines outlining the proper balance between copyright protection and the freedom to access data protected by copyright gives rise to this problem.

Moreover, in spite of continuous legislative endeavours, there is still a significant disparity between the theoretical protection mechanisms and their actual application in practise, which contributes to a general perception of regulatory ambiguity. The lack of a clear connection between the Data Act and the data reuse exception outlined in Directive (EU) 2019/790, also referred to as the Copyright Directive, adds to this uncertainty. Making sense of this relationship could be crucial to reducing or eliminating the possibility of copyright infringement lawsuits in the context of AI training, an already complex international field.

With the exception of Article 3(1), which has a one-year longer transition period, the Data Act is anticipated to take effect in the EU as of autumn 2025, having received formal approval from the European Parliament on November 9th.

How can you prepare?

The AI Act is a crucial piece of legislation that applies to all businesses that create or use artificial intelligence (including those in the deep development and testing stages), with risk and compliance officers being particularly regulated. It is imperative that these players begin evaluating their risk immediately, even if it is not final, by:

1) **Identifying the number and type of AI-based software used and developed**
For businesses to fully understand and comply with the AI Act, they must begin by conducting an extensive assessment of all of their current, upcoming, and under-development AI models, especially those that they plan to purchase from outside vendors. After this critical evaluation, every AI model ought to be painstakingly categorised in a model repository. Organisations that provide financial services in particular are in a good position to benefit from their existing model repositories. Through the incorporation of AI as an extra element into their current model governance frameworks, these entities are able to conform to the requirements of the AI Act while simultaneously preserving operational effectiveness and compliance. Businesses who haven't used a model repository yet ought to start with a status quo analysis to determine how much AI they are exposed to now and in the future.

2) **Evaluating their impact on the business model**
Analyse each AI-based software's effect on the company to determine how it affects related criticality and the company's ability to compete in the market. This includes looking into creative ways to improve or launch new services using AI within the confines of the law. For continued compliance, it is essential to set up efficient monitoring and reporting systems for AI systems and to be aware of the possible penalties and financial and reputational risks of non-compliance.

3) **Identifying the risk category each AI-based software falls in**
Using a risk-based methodology, the EU AI Act divides AI applications into four categories: low risk, high risk, limited risk, and unacceptable risk. Each category is then subject to a different level of regulation. AI with unacceptable risks, such as those that allow governments to score citizens based on their social media activity, is prohibited. High-risk artificial intelligence (AI) must abide by strict regulations, including risk assessments and transparency, in order to be used in crucial fields like infrastructure, law enforcement, and employment. Minimal risk AI systems are subject to minimal regulation, while limited risk AI systems must be transparent. The listed AI-based applications will be categorised using this system.

4) **Evaluating the activities, and costs, needed to ensure compliance**
Data governance and privacy become critical under the EU AI Act, and banks must make sure that their data practises support the Act's emphasis on ethical data sourcing and processing. In order to stop discrimination and guarantee that customers are treated fairly, ethical AI implementation is also crucial. An additional important consideration is the financial impact of complying with these regulations, which includes expenses for staff training and system upgrades.

Finally, setting up an effective monitoring and reporting mechanisms for AI systems is vital for ongoing compliance, along with understanding the financial and reputational risks associated with non-compliance, including potential penalties.

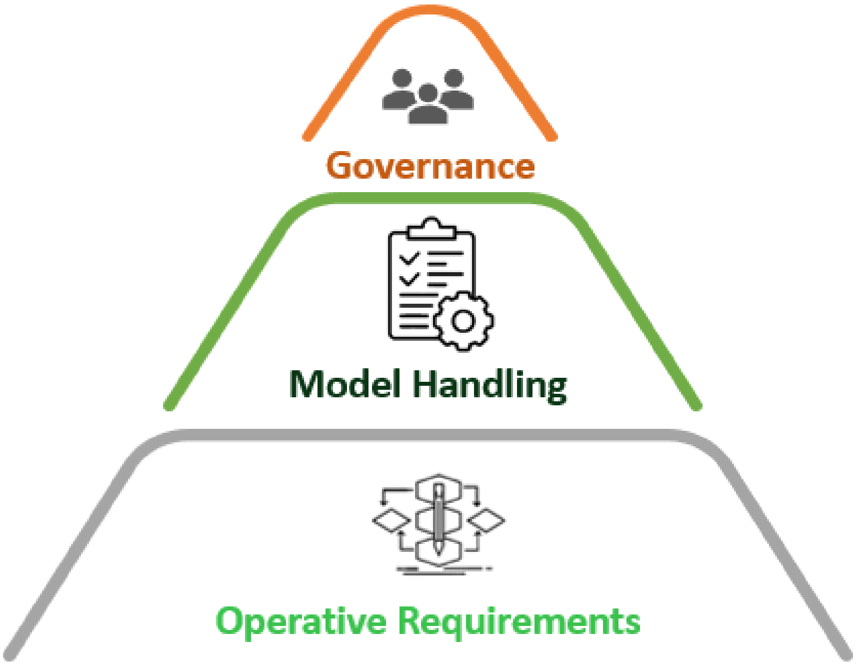
What can Avantage Reply do for you?

Avantage Reply can help you turn your vision into reality: we combine a strategic approach and a solid experience with today's cutting-edge technologies to start making things happen from day one.

We developed an extensive and modular offer called **Model Governance Service** designed, developed and provided by **Avantage Reply** for the management of projects involving complex AI models in any their aspects.

Previously, high-quality data, sophisticated algorithms, enabling technology, and development-supportive processes were critical to the success of AI projects. It is now insufficient; instead, a strategy that incorporates AI deeply into the business is required, enabling efficient communication with interested parties at all levels through the use of a framework that is well-defined and organised. In order to create AI projects with confidence and in compliance with regulations, a 360-degree approach is necessary.

All of these components are covered by the Model Governance Service approach, which is integrated into the business environment in its entirety. It is therefore organised hierarchically into 3 major macro areas:



Governance establishes an effective framework with defined roles and responsibilities for clear communication of model assumptions and limitations, as well as authority to limit model usage and monitoring risk of failures. Providers should also be able to apply and verify regulations, policies and guidelines defining rules for model development, evaluation and monitoring that will be put in place or that are already present. This phase will be in charge of integrating AI into the risk framework. It is here that the metrics for data privacy and security, explainability/transparency and fairness/bias will be defined in their specific context and then applied in the following phase, according to operative actions.

Model handling includes all the processes that concern the management of the model. In detail, the parts in this phase are:

- *Model development* is performed by Machine Learning Operations for model exploration, tuning and selection and finally evaluation, using specific metrics of this phase;
- *Model testing* applies a detailed analysis of the AI model using metrics defined by the Governance phase according to the regulation to be complied with (bias, overfitting or underfitting)
- *Model implementation* involves focusing on activities to create a model for production use, with additional solutions for robustness;
- *Model monitoring* puts in place activities to monitor the model performance according to rules defined by the Governance phase to be compliant with current regulations, internal policies and guidelines.

Operative Requirements upper phases require operative technological and functional requirements to guarantee good performances according to the specific context where the service is provided. This phase provides advisory and advanced support to satisfy any requirements.

Avantage Reply has extensive expertise in AI, IT architectures, compliance and risk management, providing customers with an integrated team to tackle the compliance problem holistically. Instead of multiple teams, each assessing a piece of the problem, we can offer teams formed by AI and risk experts, along with compliance professionals within a structured and modular service.

We can help you develop and execute a strategy to guide your company through this ground-breaking revolution!

Avantage Reply (Brussels)

Nicolas Pavlovitch
Partner
n.pavlovitch@reply.com

Gabriele Mele
Senior Consultant
ga.mele@reply.com

Giulio Soana
Senior Consultant
g.soana@reply.com

Avantage Reply (Milan)

Paolo Fabris
Partner
p.fabris@reply.it

Francesca Boccia
Senior Manager
fr.boccia@reply.it

Michele Belloli
Manager
m.belloli@reply.it