SIAPARTNERS

2021

Artificial Intelligence Act What should we learn from it?

Sophie Le Goff

Partner Compliance & Assurance

+ 33 6 15 29 31 83

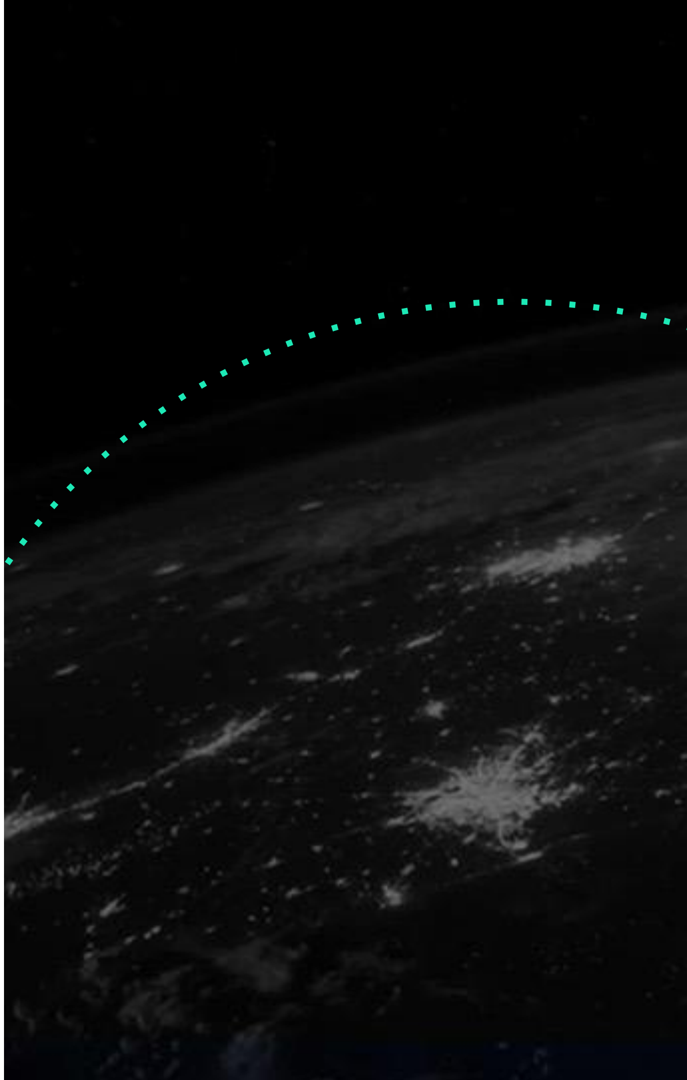
Sophie.le-goff@sia-partners.com

Jeanne Fourcade

Supervising Senior Compliance

+ 33 6 82 08 26 71

Jeanne.fourcade@sia-partners.com



Artificial Intelligence Act – Introduction

Main objectives:

Ensure that AI systems placed on the European market are safe and respect the fundamental rights of citizens and the values of the EU.

Ensure legal certainty to facilitate investment and innovation in AI.

Improve governance and effective enforcement of existing legislation on fundamental rights and safety requirements for AI systems.

Facilitate the development of a single market for legal, safe and trustworthy AI applications and prevent market fragmentation.

Fines:

Up to **2, 4 or 6% of total worldwide annual turnover**, depending on the violations foudn. Member States will be responsible for designing the sanctions regime.

Supervisory authorities:

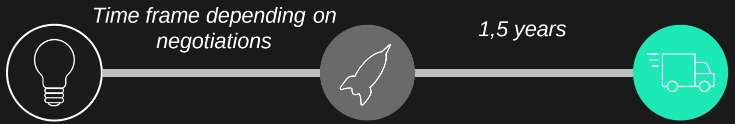
European Artifical Intelligence Board

To be determined

Targeted companies:

- Providers who distribute or offer AI systems in the Union, whether such providers are established in the Union or in a third country.
- Users of AI systems located in the Union
- Providers and users of AI systems located in a third country, when the results produced by the system are used in the Union.

Planning:



Time frame depending on negotiations

1,5 years

21/04/2021

Publication of the draft regulation

?

Parliament's vote

?

Entry into force

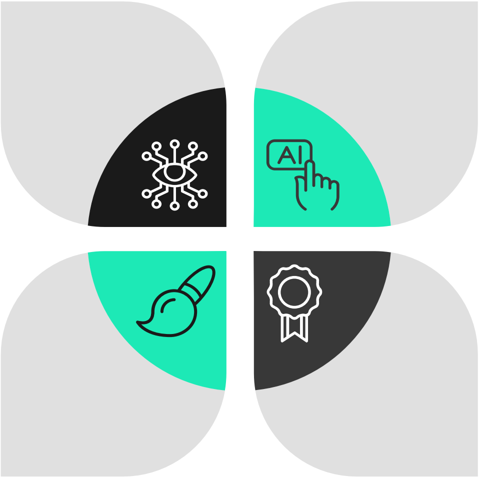
Linked regulations:

The AI Act is part of the European data package and is therefore linked to the DSA, DGA, DMA, etc. but also to the GDPR.

Artificial Intelligence Act – Key focus

RISK-BASED CATEGORY OF OBLIGATIONS

The obligations in the text depend on the risk level of the AI system used (unsustainable, high or non-high) and the actor involved (supplier, distributor, user, other third parties). There are also specific obligations for importers of high risk AI systems into the EU.



HIGH-RISK AI SYSTEMS LIST

The list of high risk systems is defined and updated by the European Commission to reflect the rapid evolution of technologies.

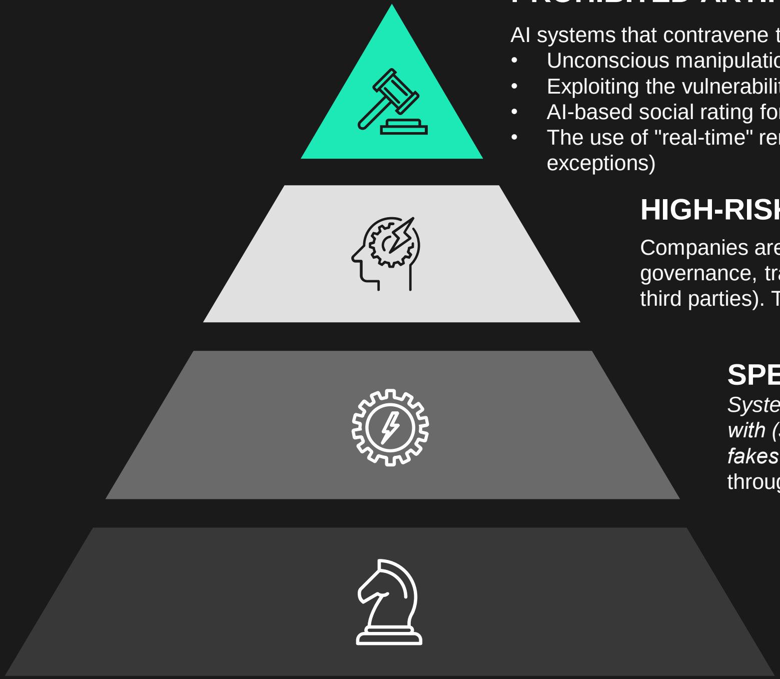
REGULATORY SANDBOXES

National competent authorities may establish regulatory sandboxes that establish a controlled environment for testing innovative technologies for a limited time. These sandboxes are based on a test plan agreed with the competent authorities to ensure compliance of the innovative AI system and to accelerate market access. SMEs and start-ups can have priority access to them.

CE MARKER & REGISTRATION

The AI Act creates a CE marker for high risk AI systems. This marker is mandatory and is provided by notified bodies. There is also an obligation to register high-risk autonomous AI systems in a European database.

Artificial Intelligence Act - Impacts



PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

AI systems that contravene the values of the European Union by violating fundamental rights are prohibited, such as:

- Unconscious manipulation of behavior
- Exploiting the vulnerabilities of certain groups to distort their behavior.
- AI-based social rating for general purposes by public authorities
- The use of "real-time" remote biometric identification systems in publicly accessible spaces for law enforcement (with exceptions)

HIGH-RISK SYSTEMS *(defined and listed by the EU Commission)*

Companies are subject to several obligations related to documentation, risk management system, governance, transparency or safety, depending on their qualification (supplier, user, distributor and other third parties). These systems must also be declared to the EU and bear a CE mark. See next page.

SPECIFIC RISK SYSTEMS

Systems that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content ('deep fakes'). For these systems, there is an obligation to **disclose** whether the content is generated through automated means or not.

NON HIGH RISK SYSTEMS

Voluntary creation and enforcement of a code of conduct that may include commitments to environmental sustainability, accessibility for people with disabilities, stakeholder participation in AI system design and development, and development team diversity.

Artificial Intelligence Act – Focus on high-risk systems (1/2)

High-risk systems areas

- Safety component of a product or the product requires a third-party conformity assessment according to existing regulations (Dir 2009/48/EC on the safety of toys, Reg 2016/424/EU on cableways, etc)

List provided in Annex III

- Biometric identification and categorisation of natural persons
- Management and operation of critical infrastructure
- Education and vocational training
- Employment, workers management and access to self-employment
- Access to and enjoyment of essential private services and public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

N.B : this list can be regularly updated by the European Commission

SYSTEMS REQUIRE-MENTS

RISK MANAGEMENT SYSTEM

Continuous iterative process run throughout the entire lifecycle of a high-risk AI system (identification, evaluation of risks and adoption and testing of risk management measures)

ACCURACY, ROBUSTNESS AND CYBERSECURITY

Implementation of measures and information in the instructions

DATA AND DATA GOVERNANCE

Training, validation and testing of data sets meeting quality criteria

HUMAN OVERSIGHT

Ensure the oversight by natural persons during the period in which the AI system is in use

TECHNICAL DOCUMENTATION

Demonstration of high-risk AI system compliance with requirements

TRANSPARENCY AND PROVISION OF INFORMATION TO USERS

Transparent design & instructions for users

RECORD-KEEPING

Design and development with capabilities enabling the automatic recording of events

Artificial Intelligence Act – Focus on high-risk systems (2/2)

	OBLIGATIONS FOR PROVIDERS	OBLIGATIONS FOR DISTRIBUTORS	OBLIGATIONS FOR USERS
GENERAL REQUIREMENTS	• Ensure that the system is compliant (see the previous page) • Take the necessary corrective actions if the high-risk AI system is not compliant	• No distribution of a non-compliant high-risk system and if the high-risk AI system is already in the market, take actions • Storage or transportation conditions must not compromise the system's compliance with requirements • Verify that the high-risk AI system bears the required CE mark of conformity	• Ensure the relevance of the data entered • Stop the use of the system if it is considered to present risks to health, safety, the protection of fundamental rights, or in the event of a serious incident or malfunction.
PROCESSES	• Have a quality management system (strategy, procedures, resources, etc.) • Write technical documentation • Conformity assessment • EU declaration and CE marking • Design and develop systems with automatic event logging capabilities • Maintain logs generated automatically by the system • Establish and document a post-market surveillance system	• Third party monitoring: to verify that the supplier and importer of the system have complied with the obligations set out in this regulation and that corrective action has been or is being taken	• Keep logs automatically generated by the system if they are under their control
TRANSPARENCY & INSTRUCTIONS	• Design transparent systems • Draft instructions for use	• Ensure that the AI system is accompanied by operating instructions and required documentation	• Obligation to use and monitor systems following the instructions of use accompanying the systems
INFORMATION & REGISTRATION	• Obligation to inform the competent national authorities in case of risks to health, safety, protection of fundamental rights or in case of serious incidents and malfunctions. • Register the system in the EU database	• Obligation to inform the supplier/importer of a non-compliant high risk system and the competent national authorities	• Obligation to inform the supplier/distributor, or the market surveillance authority, if the user cannot reach the supplier and the systems present risks to the health, safety, protection of fundamental rights of the persons concerned.