



# AI ACT: WHAT YOU (REALLY) NEED TO KNOW

11 JULY 2024

ADVANT Nctm

# THE AI ACT

## INTRODUCTION

ADVANT Nctm



# THE AI ACT

## WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence is a **technology** that makes a machine capable of simulating human cognitive functions such as perception, thinking, reasoning, and learning.

The systems to which this technology is applied are known as **artificial intelligence systems**.

Artificial intelligence systems are distinguished from other systems by their inference capability, i.e. to obtain *outputs* and derive models and/or algorithms from the received *data/input*.

They do this by using **machine learning** techniques (automatic learning) that consist of training models with (more or less) large data sets.

The most advanced *machine learning* technique is **deep learning** whose **models**, based on specific algorithmic structures called neural networks, are trained with huge unstructured data sets. *Large language models* are *deep learning* models that allow the artificial intelligence system to answer questions and generate text. They are employed by generative artificial intelligence systems such as ChatGPT.

# THE AI ACT

## WHAT IS AND WILL ARTIFICIAL INTELLIGENCE BE USED FOR?

Everyday experience already offers numerous opportunities for contact with artificial intelligence systems.

When we do a search on Google, translate a text on DeepL, or ask Siri a question, the search results, the translated text, or Siri's suggestion are all *outputs* generated by artificial intelligence systems.

But the scope of use or possible use of artificial intelligence systems is much broader: from industry to agriculture, from transport to health to the intellectual professions, including the legal professions.

The impact that artificial intelligence could have in the coming years is such that some are predicting the advent of the **fourth industrial revolution** after steam engines, electricity, and information technology.

# THE AI ACT

## WHAT ARE THE RISKS?

The large-scale use of artificial intelligence systems brings with it **significant risks**.

For the first time in history, intellectual work could be performed by machines with the consequent **disappearance of certain professional figures** and devastating consequences in terms of employment.

Then there is the question of **imputation of liability** for damages caused by artificial intelligence systems.

Not to mention the risks of **compression of freedom and fundamental** human **rights** such as the right not to be discriminated against (improperly programmed artificial intelligence systems could make discriminatory decisions), the right to the **protection of personal data** (artificial intelligence systems could unlawfully collect and process personal data), the right to **information** (artificial intelligence systems could spread false news), and the **right to competition** (in the case of concentration of technology and information in the hands of a few operators).

# THE AI ACT

## REGULATE OR NOT REGULATE?

Depending on which perspective one looks at it from, the law is perceived as both a **guarantee of protection** and a **brake on innovation**. States and supranational organisations therefore now find themselves deciding whether or not to regulate artificial intelligence.

The choice of the European Union was to **regulate artificial intelligence** through a regulation (thus directly applicable in all Member States).

This is Regulation EU 2024/1689, better known as the **Artificial Intelligence Act** or AI Act.

The AI Act is the **first law in the world** to organically regulate artificial intelligence.

Let's see when it will be applicable.

# THE AI ACT

SINCE WHEN DOES IT APPLY?



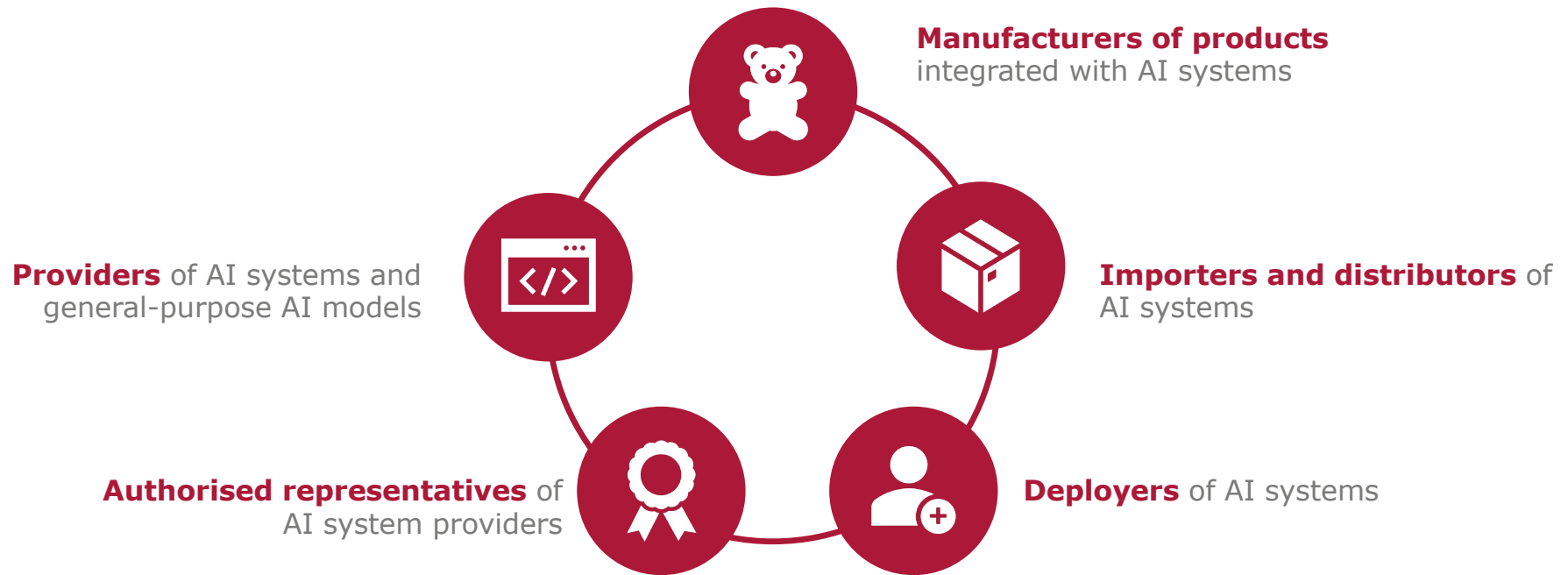
# THE AI ACT

SCOPE OF APPLICATION



# THE AI ACT

TO WHOM IT APPLIES



# THE AI ACT

## PROVIDERS

The **provider** is the natural or legal person, public authority, service or other body, established in the EU or in a third country, that develops (or has in place) an AI system or a general-purpose AI model and that:

- **places on the market** (i.e. makes available for the first time on the EU market) the AI system or general-purpose AI model or;
- **puts into service** (i.e. makes available to the deployer an AI system for use in the EU as intended) the AI system;
- does not place the AI system on the market or put it into service, but the **output generated by the system is used in the Union.**

# THE AI ACT

## AUTHORISED REPRESENTATIVES

The **authorised representative** is the natural or legal person established in the EU who has received and accepted a written **mandate** from a provider of AI systems or general-purpose AI models that is not established in the EU to perform and carry out on its behalf the obligations and procedures established in the Regulation.

The mandate must be given before the system is made available on the EU market.

The authorised representative must **withdraw** from the mandate if he believes that he is acting in violation of the Regulation.

The withdrawal and the reasons for it must be notified to the market surveillance authority of the Member State in which it is established and, where applicable, to the notified body.

# THE AI ACT

## DEPLOYER

The **deployer** is the natural or legal person, public authority, agency or other body that:

- is established in the EU and **uses** an AI system under its authority (except where the AI system is used in the course of a personal and, in any case, non-professional activity);
- is not established in the EU but the **output generated by the system is used in the EU**.

# THE AI ACT

## IMPORTERS AND DISTRIBUTORS

The **importer** is any natural or legal person established in the EU who places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

The **distributor** is any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market (i.e. provides, against payment or free of charge, for distribution or use on the EU market in the course of business).

# THE AI ACT

## MANUFACTURERS

The **manufacturer** is the natural or legal person who manufactures products integrated with AI systems that it:

- **places on the market** or
- **puts into service**

with its name or trademark.

# THE AI ACT

GENERAL-PURPOSE AI SYSTEMS AND AI  
MODELS



# THE AI ACT

## WHAT IS AN AI SYSTEM?

An AI system is a **system that uses artificial intelligence**.

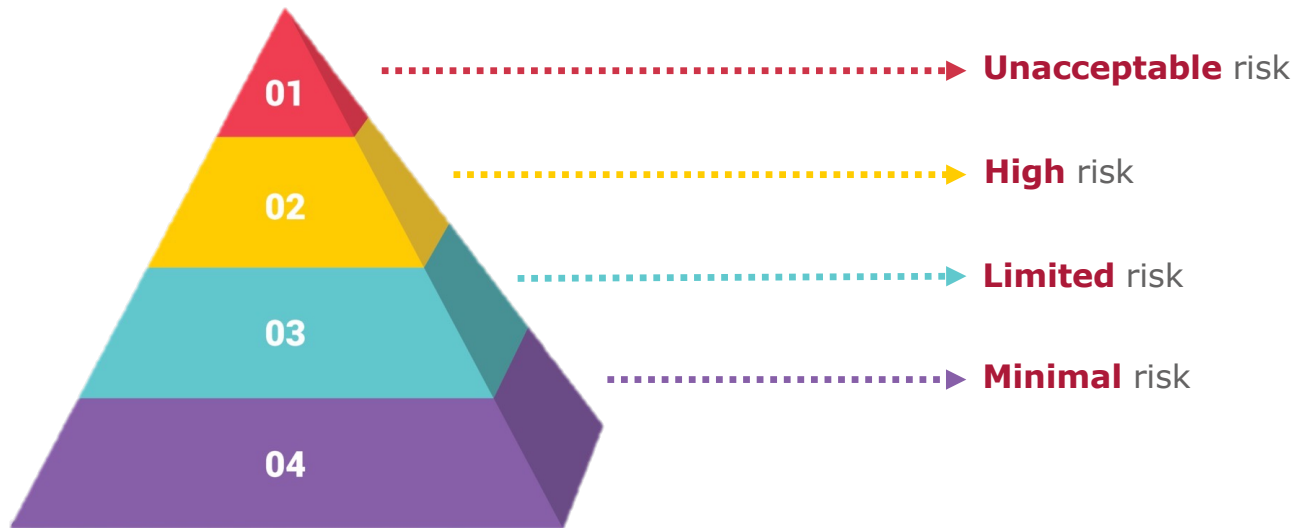
The Regulation defines it as an machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, **infers, from the input it receives, how to generate outputs** such as predictions, content, recommendations, or decisions **that can influence physical or virtual environments**.

Not all AI systems are subject to the prohibitions and conditions imposed by the Regulation, but only those that present **risks considered significant** by the European legislator.

There are **four** levels of risk.

# THE AI ACT

A RISK-BASED APPROACH



# THE AI ACT

## WHAT IS A GENERAL-PURPOSE AI MODEL?

A general-purpose AI model is defined in the Regulation as an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that is **characterised by significant generality** and is capable of competently performing a **wide range of distinct tasks**, regardless of the way the model is placed on the market, and that can be integrated into a variety of downstream systems or applications, with the exception of AI models that are used for research, development or prototyping activities before they are placed on the market.

An example of a general-purpose AI model is **GPT** (Generative Pre-trained Transformer), developed by OpenAI, which can be adapted and used for multiple purposes without having to be redefined from scratch for each of them.

# **THE AI ACT**

## PROHIBITED AI SYSTEMS

**ADVANT** Nctm



# THE AI ACT

## PROHIBITED AI SYSTEMS



**Systems using subliminal, manipulative or deceptive techniques**



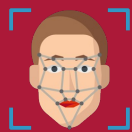
**Systems exploiting vulnerabilities**



**Social scoring systems**



**Predictive policing systems**



**Facial recognition systems based on scraping facial images**



**Emotional recognition systems in work or educational settings**



**Biometric categorisation systems according to protected or sensitive attributes**



**Real-time remote biometric identification systems in publicly accessible spaces**

# THE AI ACT

## SYSTEMS USING SUBLIMINARY, MANIPULATIVE OR DECEPTIVE TECHNIQUES

**Subliminal** techniques can be defined as those techniques that aim to influence a person's behaviour by presenting a stimulus in such a way that the person remains unaware of the presented stimulus.

**Manipulative** techniques, on the other hand, aim to change a person in a deliberate and covert manner.

**Deception**, in the context of AI systems, refers to an intentional act or omission by an AI system to create false or misleading impressions.

AI systems using these techniques are prohibited if their purpose or effect is to **significantly distort the behaviour of** a person or a group of persons, thereby impairing to the same extent their ability to make an informed decision and causing them to make a **decision they would not otherwise have made**, in a way that causes or is likely to cause that person, another person or a group of persons **significant harm**.

# THE AI ACT

## SYSTEMS EXPLOITING VULNERABILITIES

An AI system could be designed to exploit the **vulnerabilities** of a person or a specific group of persons due to:

- age (e.g. minors);
- disability; or
- social or economic situation (e.g. people in extreme poverty).

AI systems that exploit these types of vulnerabilities are prohibited if their purpose or effect is to **significantly distort the behaviour** of a person or persons belonging to a specific group of persons and cause **significant harm to** these or other persons.

# THE AI ACT

## SOCIAL SCORING SYSTEMS

*Social scoring* systems are AI systems for evaluating or ranking persons or groups of persons on the basis of their **social behaviour** or **known**, inferred or predictable **characteristics** relating to their person or personality.

*Social scoring* systems that have the effect of subjecting certain persons or groups of persons to **prejudicial or unfavourable treatment** are prohibited:

- in **social contexts** that are not related to the contexts in which the data were originally generated or collected;
- that is **unjustified or disproportionate** in relation to the social conduct engaged in or its seriousness.

# THE AI ACT

## PREDICTIVE POLICING SYSTEMS

Predictive policing systems are AI systems used to assess or predict the **risk of a specific person committing a crime**.

Predictive policing systems are prohibited if such a risk assessment is based solely on the analysis of:

- **the person's** profile; or
- the traits and characteristics of his **personality**.

The prohibition only does not apply if they are used to **corroborate evaluations made by humans** that are already based on objective, verifiable facts directly related to a criminal activity.

# THE AI ACT

## FACIAL RECOGNITION SYSTEMS BASED ON SCRAPING FACIAL IMAGES

An AI system for creating facial recognition databases uses machine learning algorithms to **collect, analyse and identify faces in images** that are then fed into structured databases.

These types of AI systems often make use of so-called **scraping**, a technique that enables the system to automatically extract data from web pages or other online sources.

AI systems that create or extend facial recognition databases by **indiscriminate** (i.e. non-targeted) **scraping** of facial images from:

- **Internet**; or from
- **CCTV systems**.

# THE AI ACT

## EMOTION RECOGNITION SYSTEMS IN WORK OR EDUCATIONAL SETTINGS

Emotion recognition systems **analyse and interpret facial expressions** in order to **identify human emotions**.

These systems are designed to detect and classify a range of emotional states, such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction, and amusement, by observing human facial features, such as eye, mouth, and eyebrow expressions.

They can be used in a variety of contexts, such as monitoring user well-being, analysing customer feedback, personalising services, and social interaction.

Emotion recognition systems are prohibited under the Regulation in the context of:

- the **workplace**;
- **educational institutions**.

This prohibition does not apply only when such systems are used for **medical or security reasons**.

# THE AI ACT

## BIOMETRIC CATEGORISATION SYSTEMS ACCORDING TO PROTECTED OR SENSITIVE ATTRIBUTES

**Biometric** data are data relating to the physical, physiological or behavioural characteristics of a person (e.g. fingerprints, iris characteristics, facial minutiae, etc.).

**Biometric categorisation** systems are those systems that use biometric data to classify the persons they refer to into categories.

Biometric categorisation systems that have the effect of classifying natural persons into categories based on:

- **race;**
- **political opinions;**
- **trade union membership;**
- **religious or philosophical beliefs;**
- **sex life or sexual orientation;**

are prohibited.

This prohibition does not apply where such systems are used for law enforcement purposes and the biometric data have been legitimately acquired.

# THE AI ACT

## REAL-TIME REMOTE BIOMETRIC IDENTIFICATION SYSTEMS IN PUBLICLY ACCESSIBLE SPACES

Real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes are, as a rule, prohibited.

Their use is permitted, to the extent strictly necessary and subject to compliance with the further conditions laid down in the Regulation (including obtaining prior authorisation from a judicial authority or an independent administrative authority), for:

- the targeted search for **victims of kidnapping, human trafficking or sexual exploitation**, as well as the search for **missing persons**;
- the prevention of a **specific**, substantial and imminent threat to life or physical integrity or the threat of a **terrorist attack**;
- locating or identifying a **person suspected of having committed a criminal offence**, within the framework of criminal proceedings in relation to offences punishable by a maximum term of imprisonment of at least four years.

# **THE AI ACT**

## HIGH-RISK AI SYSTEMS

**ADVANT** Nctm



# THE AI ACT

## WHEN IS AN AI SYSTEM HIGH-RISK?

An AI system is high-risk if it is among the high-risk AI systems listed in **Annex III** of the Regulation or, in any case, if

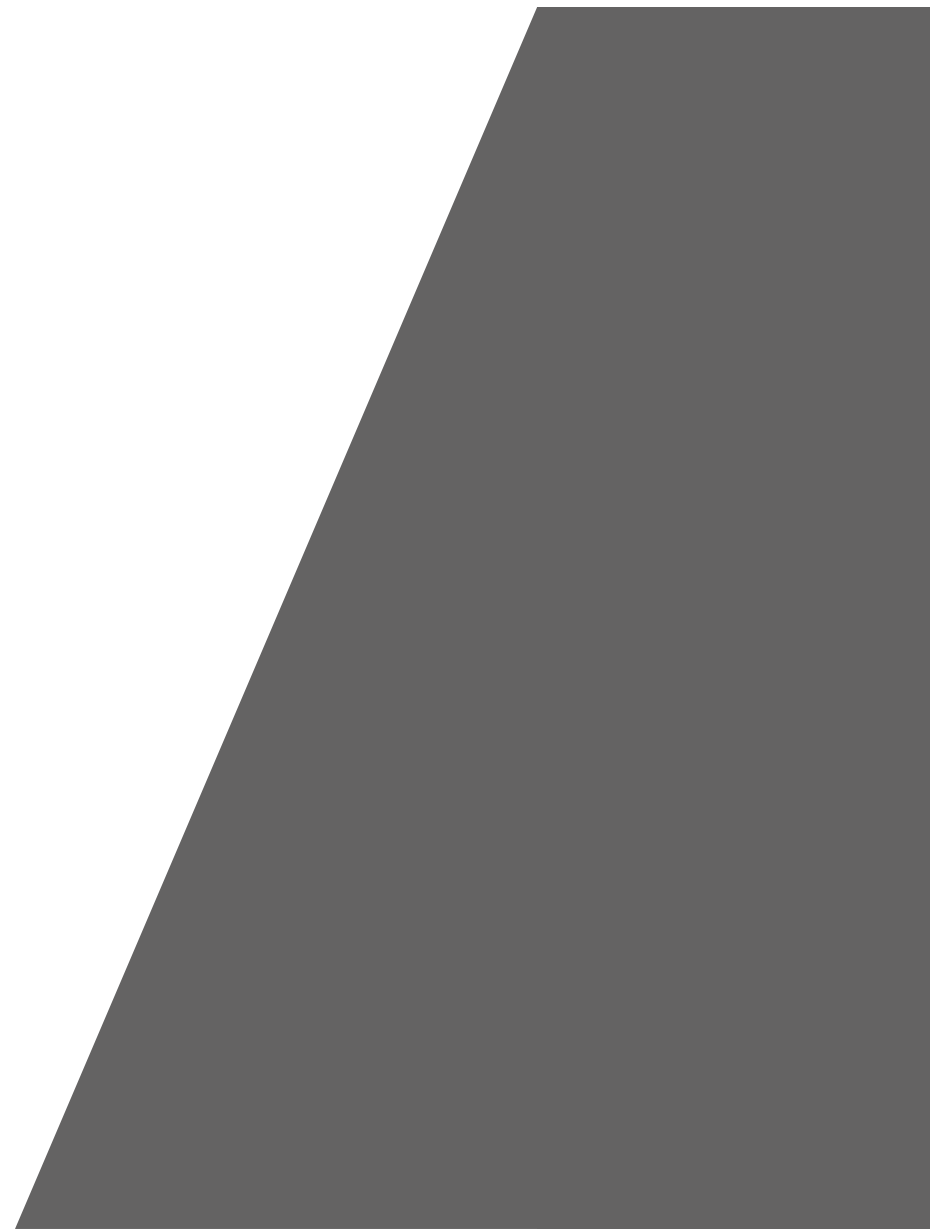
- the AI system is intended to be used as a safety component of a product or the AI system is itself a **product subject to the regulations and directives set out in Annex I** (e.g. Machinery Regulation, MDR, IVDR, etc.); and if
- the product, whose safety component is the AI system, or the AI system itself as a product, is subject to a third-party **conformity assessment for the** purpose of placing that product on the market or putting it into service.

Under certain circumstances, an AI system that is also listed in Annex III may be considered as not high risk.

The Commission may, by means of delegated acts, amend the list of high-risk AI systems in Annex III, establish new conditions for assessing the riskiness of the system, and provide guidance for the benefit of operators.

# THE AI ACT

## ANNEX III HIGH-RISK SYSTEMS



# THE AI ACT

## HIGH RISK SYSTEMS UNDER ANNEX III



**Biometrics-based  
AI systems**



**AI systems in the  
critical  
infrastructure  
sector**



**AI systems in  
education and  
vocational training**



**AI systems in work  
settings**



**AI systems for the  
access and use of  
essential services**



**AI systems for law  
enforcement  
purposes**



**AI systems in the  
field of migration,  
asylum and border  
control**



**AI systems in the  
administration of  
justice and  
democratic  
processes**

# THE AI ACT

## BIOMETRICS-BASED AI SYSTEMS

Among AI systems that rely on biometrics, the Regulation considers systems, other than those prohibited, that fall into the following categories to be high-risk:

- **remote biometric identification** systems, except for those whose sole purpose is to confirm that a particular natural person is the person he or she claims to be;
- systems intended to be used for **biometric categorisation based on the inference of protected sensitive attributes or characteristics**;
- **emotion recognition** systems.

# THE AI ACT

## AI SYSTEMS IN THE CRITICAL INFRASTRUCTURE SECTOR

Among the AI systems used in the critical infrastructure sector, the regulation considers AI systems intended for use as security components in the management and operation of:

- **critical digital infrastructure** (e.g. electronic communication networks);
- **road traffic**;
- supply of **water, gas, heating, and electricity**.

# THE AI ACT

## AI SYSTEMS IN EDUCATION AND VOCATIONAL TRAINING

Among the AI systems used in education and vocational training, the regulation considers high-risk systems the ones that are used for:

- determining **access**, admission or assignment to education and vocational training institutions;
- assessing **learning outcomes**, even if only by guiding this process, in education and vocational training institutions;
- assessing the appropriate **level of education** a person will receive or be able to access, in the context of or within a education and vocational training institution;
- monitoring and identifying **prohibited** student **behaviour** during tests in the context of or within education and vocational training institutions.

# THE AI ACT

## AI SYSTEMS IN THE WORK SETTINGS

Among the AI systems used in the employment context, the Regulation considers high-risk systems the ones that are used for:

- the **recruitment** or **selection of** personnel (in particular, to publish targeted job advertisements, analyse or filter applications, and evaluate candidates);
- **taking decisions** concerning the conditions of employment relationships or the promotion or termination of employment relationships;
- **assigning tasks** based on individual behaviour or personal traits or characteristics; and
- **monitoring and evaluating** people's **performance** and behaviour in such relationships.

# THE AI ACT

## AI SYSTEMS FOR THE ACCESS AND USE OF ESSENTIAL SERVICES

Among the AI systems used to enable citizens to access and use essential (private and public) services, the Regulation considers high-risk systems the ones that are used for:

- assessing eligibility for essential **public assistance** benefits and services, including health care services, and grant, reduce, withdraw or recover such benefits and services;
- assessing and establishing **creditworthiness** (with the exception of AI systems used to detect financial fraud);
- assessing risks and determining prices in the case of life insurance health insurance;
- evaluating and classifying **emergency calls** made to request or dispatch emergency first aid services, or prioritise the dispatch of such services, and select patients for emergency health care.

# THE AI ACT

## AI SYSTEMS FOR LAW ENFORCEMENT PURPOSES

Among the AI systems used for law enforcement purposes, the Regulation considers high-risk systems the ones that are used:

- to assess the risk of a person becoming a **victim of crime**;
- as **polygraphs** and similar instruments;
- to assess the **reliability of evidence** in criminal investigations;
- to assess the **risk of offence or recidivism**;
- to **profile** persons in the course of the detection, investigation or prosecution of crimes.

# THE AI ACT

## AI SYSTEMS IN THE FIELD OF MIGRATION, ASYLUM AND BORDER CONTROL

Among the AI systems used in the field of migration, asylum and border control management, the Regulation considers high-risk systems the ones that are used:

- as **polygraphs** or similar instruments;
- to assess a **risk** (including security risks, risks of irregular migration or health risks) posed by a person who intends to enter or has entered the territory of a Member State;
- to assist the competent public authorities in **examining** asylum, visa and residence permit applications and related complaints regarding the admissibility of persons applying for such status (including assessing the reliability of evidence);
- to locate, recognise or **identify persons** (with the exception of verification of travel documents).

# THE AI ACT

## AI SYSTEMS IN THE ADMINISTRATION OF JUSTICE AND DEMOCRATIC PROCESSES

Among the AI systems used in the administration of justice and democratic processes, the Regulation considers high-risk systems the ones that are used:

- to assist a judicial authority in **researching and interpreting** facts and law and applying law to a set of facts or used in a similar way in alternative dispute resolution;
- to influence **the outcome of an election or referendum or the voting behaviour** of people when exercising their vote in elections or referendums.

# THE AI ACT

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS



# THE AI ACT

## REQUIREMENTS FOR HIGH-RISK SYSTEMS



**Risk Management System**



**Procedures to ensure data quality**



**Technical Documentation**



**Record keeping**



**Instructions for use**



**Human oversight**



**Accuracy, robustness and cybersecurity**

# THE AI ACT

## RISK MANAGEMENT SYSTEM

A risk management system is a set of processes, procedures and tools designed to **identify, assess and manage**, on an ongoing basis and throughout the life cycle of high-risk AI systems, the **risks** that the systems pose to **health, safety and fundamental rights**.

Identified risks must be managed through the adoption of **risk management measures**.

Risk management measures must make it possible to:

- **contain the residual risk** associated with each risk (and the overall residual risk of the high-risk AI system) to an acceptable level;
- ensure, to the extent technically feasible, the **elimination or reduction of identified risks** through appropriate design and development of the high-risk AI system;
- where necessary, ensure the **mitigation and monitoring of risks** that cannot be eliminated;
- ensure that **operating instructions** are provided to deployers and that they are given any necessary **training**.

In order to identify the most appropriate risk management measures, high-risk AI systems are subject to tests, which are to be carried out before they are placed on the market or put into service.

# THE AI ACT

## PROCEDURES TO ENSURE DATA QUALITY

The sets of data (personal and non-personal) used for training, validating, and testing the models on which high-risk AI systems are based must be subject to **procedures to ensure data quality**, taking into account, in particular:

- the relevant **design choices**;
- the **data collection processes** and their **source** (and, in the case of personal data, the original purpose of collection);
- processing activities for data **preparation** (e.g. labelling, cleaning, updating, etc.);
- the formulation of **assumptions**, particularly with regard to the information that the data should measure and represent;
- the **availability, quantity** and **adequacy** of the necessary data sets;
- **possible errors** that could affect people's health and safety, adversely affect fundamental rights or lead to discrimination prohibited by EU law;
- appropriate **measures** to detect, prevent and mitigate possible errors;
- how to **identify (and remedy)** data **gaps and deficiencies** that prevent full compliance.

# THE AI ACT

## TECHNICAL DOCUMENTATION

The conformity of high-risk AI systems with the requirements of the Regulation must be documented by means of technical documentation. The technical documentation must contain at least:

- a **general description of the** high-risk AI **system**;
- a **detailed description of the elements of the** high-risk AI **system** and the development process;
- detailed information on the **monitoring, operation and control** of the high-risk AI system;
- a **description of the adequacy of performance metrics** for the specific high-risk AI system;
- a **detailed description of the risk management system**;
- a description of the **relevant changes made by the provider** to the high-risk AI system during its life cycle;
- the list of **harmonised standards applied** (in whole or in part);
- a copy of the **declaration of conformity**;
- a detailed description of the system in use to assess the **performance of the** high-risk AI **system** in the post-marketing phase.

# THE AI ACT

## RECORD KEEPING

High-risk AI systems must allow **automatic logging** throughout the system's life cycle. In particular, logs must be registered when they are used to:

- detect those situations from which a risk or substantial change may arise;
- facilitate post-marketing monitoring;
- monitor the functioning of the system.

**Remote biometric identification systems** must record the date and time and the end date and time of each use, the reference database against which the input data has been checked by the system, the input data for which the search has led to a match, and the identity of the natural persons involved in the verification of the results.

# THE AI ACT

## INSTRUCTIONS FOR USE

High-risk AI systems must be accompanied by operating instructions for the deployers. The operating instructions must at least contain information about:

- the **identity and contact details of the provider** and, if applicable, of the authorised representative;
- the **characteristics, potential** and **performance limits** of the system, including the intended use, the level of accuracy, the circumstances from which risks may arise, the ability of the system to provide useful information to explain its outputs, the performance in relation to persons or groups of persons for whom the system is intended, information on datasets and on training, validation and testing of them, and information to enable deployers to correctly interpret and use the outputs;
- any **changes** to the high-risk AI system and its performance predetermined by the provider at the time of the initial conformity assessment;
- human **supervision** measures, including those to facilitate the interpretation of outputs by deployers;
- the necessary computational and hardware **resources**, the expected **lifetime** of the system and measures for system **maintenance** and protection;
- the description of mechanisms enabling deployers to collect, store, and correctly interpret **logs**.

# THE AI ACT

## HUMAN OVERSIGHT

High-risk AI systems must be able to be supervised by physical persons. High-risk AI systems must therefore provide for **human oversight measures** that enable the deployer to:

- understand the functionality and limitations of the system and monitor its operation;
- be aware that the system may lead them to rely automatically or to over-rely on the results produced;
- correctly interpret the results of the system;
- decide, in particular situations, not to use the system or to disregard, ignore or reverse the results of the system;
- intervene in system operation or shut down the system via a 'stop' button or similar procedure.

**Biometric remote identification systems** must additionally provide for human oversight measures to ensure that no action or decision is taken by the deployer on the basis of the identification resulting from the system unless it has been verified and confirmed separately by at least two natural persons with the necessary competence, training and authority.

# THE AI ACT

## ACCURACY, ROBUSTNESS AND CYBERSECURITY

High-risk AI systems must be designed and developed to maintain an adequate level of accuracy, robustness and cybersecurity throughout the system's life cycle.

The level of **accuracy** must be indicated in the operating instructions.

In order to ensure an adequate level of **robustness**, technical measures (e.g. backups) must be taken to make the system as resilient as possible to possible errors, failures or inconsistencies, eliminating or reducing, in the case of systems that continue to learn after being placed on the market or put into service, the risk that the results may condition the inputs for future operations (so-called 'feedback loops').

To ensure an adequate level of **cybersecurity**, measures must be taken to prevent, detect and react to cyber attacks that exploit system vulnerabilities (e.g. data poisoning, model poisoning, adversarial examples, model evasion, etc.).

# **THE AI ACT**

## OBLIGATIONS OF PROVIDERS



# THE AI ACT

## OBLIGATIONS OF PROVIDERS



**Compliance  
with high-risk  
AI systems  
requirements**



**Labelling**



**Quality  
management  
system**



**Technical  
documentation  
retention**



**Record keeping**



**Conformity  
assessment**



**Registration of  
high-risk AI**



**Withdrawal,  
recall and  
reporting  
obligations**



**Regulatory  
cooperation**

# THE AI ACT

## OBLIGATIONS OF PROVIDERS

The provider must:

- ensure that **the system meets the requirements** of high-risk AI systems (as well as accessibility requirements);
- indicate on the system or at least on the packaging or accompanying documentation its **name**, registered trade name or trademark and the **address** at which it can be contacted;
- adopt a **quality management system**;
- keep the **system documentation** (technical documentation, declaration of conformity, etc.) for 10 years;
- keep the **logs** automatically generated by the system for at least 6 months;
- submit the system to the relevant **conformity assessment** procedure, draw up the **declaration of conformity**, and affix the **CE mark** on the system or at least on the packaging or accompanying documentation;
- register themselves and the system in the **EU database** (in cases where registration is mandatory);
- take the **necessary corrective measures** (including withdrawal and recall) and comply with reporting obligations;
- **demonstrate** the compliance of the system if requested to do so by the market surveillance authority.

**ADVANT** Nctm

# THE AI ACT

## QUALITY MANAGEMENT SYSTEM

The function of the quality management system is to **ensure compliance** with the Regulation. The quality management system must include, among others:

- a **strategy** for regulatory compliance;
- the **procedures** to be followed in the design, development, examination, testing and validation phases;
- the **data management** systems and procedures;
- the **risk management** system;
- the **monitoring system** after its placing on the market;
- the procedures related to the **reporting of serious incidents**;
- the management of the **communication** with national competent authorities, notified bodies, other operators, deployers or other interested parties;
- the systems and procedures for keeping **logs** and all relevant information and documentation;
- the **resource management**, including measures relating to security of supply;
- the definition of **roles and responsibilities** within the organisation.

# THE AI ACT

OBLIGATIONS OF AUTHORISED  
REPRESENTATIVES



# THE AI ACT

## OBLIGATIONS OF AUTHORISED REPRESENTATIVES

The authorised representative must perform the tasks specified in the mandate given to him by the provider. The mandate must empower the authorised representative to:

- verify that the provider has drawn up the EU **declaration of conformity and the technical documentation** and has carried out the **conformity assessment**;
- keep (for at least 10 years from the date of placing on the market or putting into service) and make available to the competent national authorities the **provider's contact details** and a **copy of the EU declaration of conformity**, the **technical documentation** and, if applicable, the **certificate of conformity** issued by the notified body;
- provide the competent national authorities, upon request, with the information and documents necessary to **demonstrate** the compliance of the high-risk AI system with the Regulation (including the logs automatically generated by the system in the provider's possession);
- **cooperate** with the competent national authorities in connection with decisions taken by them;
- if applicable, fulfil **registration** obligations.

# **THE AI ACT**

## OBLIGATIONS OF IMPORTERS



# THE AI ACT

## OBLIGATIONS OF IMPORTERS

The importer must:

- prior to placing a high-risk AI system on the market, check that the provider has carried out the **conformity assessment**, drawn up the **technical documentation** and designated an **authorised representative**, and that the AI high-risk system bears the **CE mark** and is accompanied by the EU **declaration of conformity** and **operating instructions**;
- **not to place** the high-risk AI system on the market if it believes that it does not comply with the Regulation, informing the authorised representative and the market surveillance authority in case of risk;
- indicate on the system or at least on the packaging or accompanying documentation its **name**, registered trade name or trademark and the **address** at which it can be contacted;
- ensure that **storage and transport conditions** do not compromise the compliance of the high-risk AI system with the Regulation;
- keep (for 10 years from the date of placing on the market) the EU **declaration of conformity**, the **operating instructions** and, if applicable, the **certificate of conformity** issued by the notified body;
- **provide the** competent national authorities, upon request, with the information and documents necessary to demonstrate the compliance of the AI system with the Regulation;
- **cooperate** with the competent national authorities in relation to the decisions taken by them.

**ADVANT** Nctm

# THE AI ACT

## OBLIGATIONS OF DISTRIBUTORS



# THE AI ACT

## OBLIGATIONS OF DISTRIBUTORS

The distributor must:

- before the high-risk AI system is made available on the market, check that it bears the **CE marking** and is accompanied by the EU **declaration of conformity** and **operating instructions**, and that the provider and importer (if any) have indicated its **name**, trade name or trademark and **address**;
- **not make** the high-risk AI system **available** on the market if it believes it does not comply with the Regulation, informing the provider and importer (if any) in the event of risk;
- ensure that **storage and transport conditions** do not compromise the AI system's compliance with the Regulation;
- if it considers that the high-risk AI system (already made available on the market) is not compliant with the Regulation, **take the necessary corrective action** to bring the system into compliance, withdraw it from the market or recall it, or otherwise ensure that such corrective action is taken by the provider or importer (if any), informing the provider, the importer (if any) and the competent national authorities in case of risk;
- **provide** the competent national authorities, upon request, with the information and documents necessary to demonstrate compliance of the high-risk AI system with the Regulation;
- **cooperate** with the competent national authorities in relation to the decisions taken by them.

# **THE AI ACT**

## OBLIGATIONS OF DEPLOYERS



# THE AI ACT

## OBLIGATIONS OF DEPLOYERS



**Follow  
instructions for  
use**



**Assign human  
oversight**



**Relevant &  
representative  
input data**



**Monitoring &  
incident  
reporting**



**Maintain AI  
systems logs &  
records**



**Employer must  
inform workers  
about high-risk  
AI use**



**Notice &  
disclosure for  
AI decision-  
making**



**Regulatory  
cooperation**



**Fundamental  
rights impact  
assessment**

# THE AI ACT

## DUTIES OF DEPLOYERS

The deployer must:

- adopt and implement technical and organisational measures to ensure that the system is **used in accordance with the operating instructions**;
- assign human supervision to natural persons with the necessary **competence, training** and **authority** and the necessary support;
- ensure that the input **data** are **relevant and representative** in light of the intended purpose;
- **monitor** the operation of the system and **report** to provider, importer, distributor as well as to the market surveillance authority if the system presents a risk (simultaneously suspending the use of the system) as well as any serious incidents of which it becomes aware;
- **keep the logs** automatically generated by the system for at least 6 months;
- **inform workers' representatives and workers** who are subject to the use of the high-risk AI system;
- in the case of high-risk AI systems that make decisions or assist in making decisions affecting natural persons, **inform** them that they are subject to the use of the high-risk AI system;
- **cooperate** with the competent national authorities in relation to the decisions taken by them;
- in case of certain AI systems, carry out a **fundamental rights impact assessment**.

# THE AI ACT

## FUNDAMENTAL RIGHTS IMPACT ASSESSMENT

The obligation to carry out a fundamental rights impact assessment concerns:

- deployers of high-risk AI systems that are **bodies governed by public law or private entities providing public services**;
- deployers of AI systems to evaluate the **creditworthiness** of natural persons or to establish their **credit score**;
- deployers of AI systems for risk assessment and pricing in relation to natural persons in case of **life** and **health insurance**.

In the assessment, the deployer must take into account, among other things, the scope of use of the system, the time and frequency of use, the categories of natural persons affected, the risks to fundamental rights, the measures to be taken if the risks materialise, etc.

Once the assessment has been carried out, the deployer **notifies** the results to the market surveillance authority.

# THE AI ACT

CONFORMITY ASSESSMENT,  
DECLARATION OF CONFORMITY, CE  
MARKING AND REGISTRATION

**ADVANT** Nctm



# THE AI ACT

## WHAT IS CONFORMITY ASSESSMENT?

Conformity assessment is the activity of demonstrating the **conformity of a product with the requirements** of EU legislation.

Already provided for in relation to certain products, it is required by the Regulation for **high-risk AI systems**.

Through the conformity assessment, the compliance of a high-risk AI system with the requirements of the Regulation for this type of system (i.e. risk management system, procedures to ensure data quality, technical documentation, log recording, user instructions, human oversight, accuracy, robustness and cybersecurity) is evaluated.

It must be carried out **before the** high-risk AI system is placed on the **market or put into service**.

There are two procedures for conformity assessment: a **simplified** and an **ordinary one**.

# THE AI ACT

## THE SIMPLIFIED CONFORMITY ASSESSMENT

The simplified conformity assessment is that provided for in Annex VI to the regulation.

It is required for high-risk AI systems:

- referred to in point 1 of Annex III (i.e. **high-risk AI systems based on biometrics**) where the provider has implemented **harmonised standards or common specifications**;
- referred to in points 2 to 8 of Annex III (i.e. high-risk IA systems in the following areas: **critical infrastructure; education and vocational training; employment; law enforcement; migration, asylum and borders control; administration of justice and democratic processes**).

The simplified conformity assessment is carried out by the **without the involvement of a notified body** and is based on **internal control** of the quality management system, the technical documentation, the system design and development process and the post-marketing monitoring process.

# THE AI ACT

## THE ORDINARY CONFORMITY ASSESSMENT

The ordinary conformity assessment is that provided for in Annex VII of the Regulation.

It is required for high-risk AI systems referred to in point 1 of Annex III (**high-risk AI systems based on biometrics**) in the case where

- **no harmonised standards exist** and no common specifications are available;
- the provider **has not applied or has only partially applied the harmonised standards**;
- **common specifications exist but the provider has not applied them**;
- one or more harmonised standards have been published with a **restriction** and only on the part of the standard that has been limited.

# THE AI ACT

## CONFORMITY ASSESSMENTS PROVIDED FOR BY OTHER EU ACTS

For **high-risk AI systems subject to the directives and regulations in Section A of Annex I** (e.g. Machinery Regulation, MDR, IVDR, etc.), compliance with the requirements of the Regulation is assessed on the basis of the conformity assessment procedures set out in those directives and regulations.

Exemptions from the obligation to carry out a conformity assessment under these directives and regulations only apply if the provider of the high-risk AI system has applied **harmonised standards** or, where applicable, **common specifications**.

# THE AI ACT

## THE CONFORMITY CERTIFICATE

The conformity certificate is the document issued by the **notified bodies** (involved in ordinary conformity assessment as well as in conformity assessments under other EU acts) certifying the successful outcome of the conformity assessment.

The certificate must be drafted in a language easily understandable by the relevant authorities of the Member State where the notified body is established.

The validity of the certificate may not exceed **5 years for high-risk AI systems** subject to other EU acts and **4 years** for high-risk AI systems listed in Annex III, and may be extended for a further 5 and 4 years following a re-assessment.

If the notified body considers that the high-risk AI system in respect of which it has issued a certificate no longer meets the requirements set out in the regulation, it may **suspend or withdraw** the certificate and impose restrictions.

# THE AI ACT

## THE DECLARATION OF CONFORMITY

The EU Declaration of Conformity is the **document by which the provider declares**, taking responsibility for it, **that the high risk AI system complies with** the requirements of the regulation.

The EU Declaration of Conformity must be drawn up in machine-readable format, translated into the languages of the Member States in which the AI high-risk system was placed on the market or made available, must contain the information listed in Annex V and must be signed by the provider.

It must be kept for **10 years** from the date the high-risk AI system is placed on the market or put into service and be provided to the competent national authorities upon request.

For high-risk AI systems subject, in addition to the regulation, to other EU acts requiring a declaration of conformity, a single declaration of conformity must be drawn up.

# THE AI ACT

## THE CE MARKING

High-risk AI systems must be **CE-marked**.

In the case of high-risk AI systems in digital format, a digital CE marking must be affixed (provided that the marking is easily accessible through the system interface).

If it is not possible to affix the CE marking to the high-risk AI system, it must be affixed to the **packaging** or **accompanying documentation**.

If a notified body was involved in the conformity assessment procedure, the CE marking must be followed by the identification number of the notified body.

# THE AI ACT

## REGISTRATION

High-risk AI systems, with the exception of high-risk AI systems used in the critical infrastructure sector, must be registered in the **EU database** by providers or authorised representatives (who must also register).

Some sections of the EU database are **excluded from public access**. In these sections, high-risk AI systems used in the areas of law enforcement, migration, asylum and borders control management are recorded.

High-risk AI systems used in the critical infrastructure sector are registered in **national databases**.

# THE AI ACT

TRANSPARENCY OBLIGATIONS FOR  
PROVIDERS AND DEPLOYERS OF  
CERTAIN AI SYSTEMS



# THE AI ACT

## AI SYSTEMS INTERACTING WITH NATURAL PERSONS

Providers of AI systems intended to **interact directly with natural persons** must ensure that the system is designed and developed in such a way that the natural persons concerned are **informed that they** are interacting with an AI system.

This is unless the fact that one is interacting with an AI system is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.

This obligation does not apply to AI systems authorised by law to detect, prevent, investigate or prosecute crimes, subject to appropriate protections for the rights and freedoms of third parties, unless such systems are available for the public to report a crime.

# THE AI ACT

## AI SYSTEMS THAT GENERATE CONTENT

Providers of AI systems, including general-purpose AI systems **that generate** synthetic audio, image, video or text **content**, ensure that the outputs of the AI system are **marked** in a machine-readable format and detectable as artificially generated or manipulated.

Providers shall ensure that their **technical solutions** are **effective, interoperable, robust and reliable** as far as this is technically feasible, taking into account the specificities and limitations of the various types of content, the costs of implementation and the generally acknowledged state of the art, as may be indicated in relevant technical standards.

This obligation does not apply if the AI systems perform a standard editing assistance function or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute crimes.

# THE AI ACT

## AI SYSTEMS FOR EMOTION RECOGNITION AND BIOMETRIC CATEGORISATION

Deployers of an emotion recognition system or biometric categorisation system shall **inform** natural persons exposed thereto of the **operation** of the system and process personal data in accordance with applicable data protection legislation.

This obligation does not apply to AI systems used for biometric categorisation and emotion recognition authorised by law to detect, prevent or investigate crimes, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law.

# THE AI ACT

## AI SYSTEMS GENERATING DEEP FAKES

A **deep fake** is an image or audio or video content generated or manipulated by AI that resembles an existing person, object, place or other entity or event and that would appear falsely authentic or truthful to a person.

Deployers of an AI system that generates or manipulates images or audio or video content that constitutes a deep fake shall **disclose that the content has been artificially generated or manipulated**.

This obligation does not apply if the use is authorised by law to detect, prevent, investigate or prosecute crimes.

Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations referred to in this paragraph shall be limited to the obligation to disclose the existence of such content that has been generated or manipulated in an appropriate manner, without hampering the display or enjoyment of the work.

Deployers of an **AI system that generates or manipulates published text for the purpose of informing the public** about matters of public interest shall disclose that the text has been artificially generated or manipulated.

This obligation does not apply if the use is authorised by law to detect, prevent, investigate or prosecute crimes or if the AI-generated content has **undergone a human review or editorial control process and a natural or legal person holds editorial responsibility for the publication of the content**.

# **THE AI ACT**

## GENERAL-PURPOSE AI MODELS

**ADVANT** Nctm



# THE AI ACT

## GENERAL-PURPOSE AI MODELS WITH SYSTEMIC RISK

A general-purpose AI model is classified as a general-purpose AI model with **systemic risk** if:

- has **high impact capabilities**, i.e. the cumulative amount of the calculation used for its training measured in FLOPS (floating point operations per second) is greater than  $10^{25}$ ;
- is **classified as such** by **the Commission** in its decision.

The Commission's decision may be taken *ex officio* or at the outcome of a procedure starting with the notification by the general-purpose model provider that the threshold has been exceeded.

# THE AI ACT

## OBLIGATIONS OF PROVIDERS

Provider of general-purpose AI models must:

- draw up (and keep updated) in accordance with Annex XI the **technical documentation** of the model;
- make available to AI system providers who intend to integrate the model into their AI systems the **information** and **documentation** necessary to understand the capabilities and limitations of the model and to enable them to fulfil their obligations and, in any case, the information and documentation provided for in Annex XII;
- define and implement **policies** to comply with EU copyright law;
- draw up and make available to the public a **summary of the content used to train the model**;
- **cooperate** with the Commission and the competent national authorities.

In addition to the above obligations, providers of general-purpose AI models with systemic risk must

- **assess and mitigate systemic risks** arising from the development or use of the model;
- document and report **serious incidents** to the AI Office and the competent national authorities;
- ensure an adequate level of **cybersecurity**.

# THE AI ACT

## OBLIGATIONS OF AUTHORISED REPRESENTATIVES

If they are established in a third country, the providers of general-purpose AI models must appoint an authorised representative in the EU by means of a written mandate. The mandate must enable the authorised representative to:

- verify that the **technical documentation** has been drawn up and that the providers' **obligations** have been fulfilled;
- keep the technical documentation for **10 years** from the date on which the general purpose model was placed on the Union market;
- make available to the AI Office and the competent national authorities the technical documentation and the information and documentation necessary to **demonstrate compliance** with the Regulation;
- **cooperate** with the AI Office and with the competent national authorities in relation to the action taken by the latter with regard to general-purpose models with systemic risk (including when such models are integrated into AI systems placed on the market and put into service in the Union).

# **THE AI ACT**

MEASURES IN SUPPORT OF INNOVATION

**ADVANT** Nctm



# THE AI ACT

## AI REGULATORY SANDBOX

Each Member State must establish at least one **AI regulatory sandbox**.

The regulatory sandbox is a **controlled environment** in which AI systems can be developed, trained, tested and validated on the basis of a plan agreed between the AI system provider (or potential AI system provider) and the competent authority.

The competent authority shall issue the providers, upon request, with **written proof** of successful activities and an **exit report** detailing the activities carried out and the results achieved.

The written proof and exit report may be used by the AI system provider as part of the conformity assessment procedures.

# THE AI ACT

## TESTING IN REAL WORLD CONDITIONS OUTSIDE AI REGULATORY SANDBOX

To be able to carry out **tests in real world conditions**, the providers of high-risk AI systems must:

- draw up a **testing plan** in real world conditions and submit it to the market surveillance authority of the Member State where the tests are to be carried out for approval;
- **record the written proof** in the non-public part from the Union database;
- be **established in** the Union or have appointed an **authorised representative** in the Union;
- **not to transfer the data collected and processed** during the tests **to third countries**, except in accordance with Union law;
- carry out the **tests for as long as strictly necessary** and, in any case, for no longer than 6 months, extendable by a further 6 months;
- obtain the **informed consent** of the persons concerned and ensure adequate protection for vulnerable persons;
- conclude an agreement with the potential deployer involved to define their respective **responsibilities**;
- supervise the tests by **qualified personnel**;
- ensure that the predictions, recommendations and decisions of the AI system can be **ignored and overturned**.

**ADVANT** Nctm

# THE AI ACT

## GOVERNANCE

ADVANT Nctm



# THE AI ACT

## AI OFFICE

The European Artificial Intelligence Office (or, as it is better known, the **AI Office**) has been established by the European Commission with decision of 24 January 2024 (whose effectiveness was postponed to 24 February 2024).

The AI Office is part of the Directorate-General for Communication Networks, Content and Technologies (CNECT).

The AI Office was assigned, in particular, with the **control of AI general-purpose models**. As part of this activity, the AI Office:

- identifies methodologies and benchmarks to assess the capability of general-purpose models;
- monitors the application of the rules on general-purpose models and the systems that use them and investigates possible violations;
- detects any unforeseeable risks in connection with the use of general-purpose models.

It also performs **support functions for the Commission** to contribute to the effective implementation and uniform application of the AI Act.

# THE AI ACT

## EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

The **European Artificial Intelligence Board** is composed of one representative per Member State. The European Data Protection Supervisor and the AI Office also participate in its meetings, without voting rights.

Within it, two permanent subgroups are established, one of which is dedicated to **fostering cooperation and the exchange of information between national market surveillance authorities**.

It has the task, among others, of:

- contributing to the **coordination** of the competent national authorities;
- **sharing** knowledge and best practices;
- providing **advice**;
- contributing to the **harmonisation of administrative practices**;
- formulating **recommendations and opinions**.

# THE AI ACT

## ADVISORY FORUM

The **Advisory Forum** is set up by the Commission and consists of representatives of the main stakeholder groups in the field of artificial intelligence: industry, start-ups, SMEs, civil society and academia.

It has the task of:

- drafting **opinions, recommendations and other written contributions** at the request of the EAIB or the Commission;
- setting up temporary sub-groups to examine **specific questions**;
- preparing an **annual**, publicly accessible **report** on its activities.

# THE AI ACT

## SCIENTIFIC PANEL OF INDEPENDENT EXPERTS

The **Scientific Panel** is set up by the Commission and is composed of experts with scientific or technical expertise in the field of artificial intelligence and who are independent of any provider of AI systems or general-purpose AI models.

It provides **support to the AI Office** in the performance of its tasks.

Member States can also avail themselves of the support of the Scientific Panel.

# THE AI ACT

## NATIONAL COMPETENT AUTHORITIES

Each Member State shall establish or designate:

- a **notifying authority**; and
- a **market surveillance authority**.

The notifying authority is the national authority responsible for establishing and carrying out the necessary procedures for the assessment, designation and notification of notified bodies and for their monitoring.

The market surveillance authority is the authority responsible for market surveillance in the territory of the Member State.

# THE AI ACT

EU DATABASE OF HIGH-RISK AI  
SYSTEMS

ADVANT Nctm



# THE AI ACT

## EU DATABASE OF HIGH-RISK AI SYSTEMS

The Commission, in cooperation with the Member States, establishes and maintains the **EU database** for high-risk AI systems, which contains the information that Annex VIII requires providers and deployers of such systems to enter.

Relevant experts should be consulted for the development and updating of the **technical functionalities** of the database.

The information contained in the database should be **publicly accessible** (with specific exceptions) in a user-friendly manner with machine-readable format.

Any personal data contained in the European database are collected and processed to the extent strictly necessary (e.g. names and contact details of persons responsible for registration).

The **Commission** was identified as:

- data controller of the database;
- in charge of providing technical and administrative support to providers and deployers.

# THE AI ACT

POST-MARKET MONITORING,  
INFORMATION SHARING AND MARKET  
SURVEILLANCE

ADVANT Nctm



# THE AI ACT

## POST-MARKET MONITORING SYSTEM

Providers of high-risk AI systems must set up a **post-market monitoring system**.

Through the post-market monitoring system, **data on the performance** of high-risk AI systems are collected and analysed throughout their life cycle. This is done in order to **assess the compliance** of high-risk AI systems with the requirements of the Regulation **over time**.

The post-market monitoring system is based on a **monitoring plan** defined along the lines of the model monitoring plan adopted by the Commission in its decision.

For high-risk AI systems subject to the directives and regulations listed in Section A of Annex I (e.g. Machinery Regulation, MDR, IVDR, etc.), where these directives and regulations already provide for a monitoring system and plan, providers may supplement existing monitoring systems and plans with the additional elements provided for in the Regulation (and the model monitoring plan adopted by the Commission).

# THE AI ACT

## SHARING OF INFORMATION ON SERIOUS INCIDENTS

Providers of high-risk AI systems must **report any serious incident** to the supervisory authority of the Member State where the incident occurred whenever it is caused by a high-risk AI system or whenever the causal link is reasonably probable.

A serious incident is defined as an accident or malfunction of an AI system that directly or indirectly causes:

- the **death** of a person or serious damage to a person's health;
- a serious and irreversible **disruption** of the management or operation of critical infrastructure;
- **infringements** of obligations under EU law to protect fundamental rights;
- serious **damage** to property or the environment.

# THE AI ACT

## REPORTING DEADLINES

The report must be made immediately and in any case no later than **15 days** after the provider or deployer becomes aware of the incident. The 15-day period is reduced to:

- **2 days** where the serious incident has caused a serious and irreversible disruption of the management or operation of critical infrastructure;
- **10 days** if the serious incident caused the death of a person.

If complete information is not available by the deadline, the report may be completed with the missing information even after the deadline.

# THE AI ACT

## POST-REPORTING ACTIVITIES

After reporting, the provider:

- carries out the necessary **investigations**;
- **cooperate** with the market surveillance authority;
- take **corrective measures**;
- refrain from making **changes** to the high-risk AI system that prevent or compromise the assessment of the causes of the incident without first informing the supervisory authority.

The market surveillance authority:

- in the event that the incident has led to the infringement of obligations under EU law protecting fundamental rights, it **informs** the national public authorities or bodies entrusted with the supervision of compliance with those obligations;
- within 7 days of receipt of the notification, take the **appropriate measures** referred to in Article 19 of EU Regulation 2019/1020 (Regulation on market surveillance and compliance of products).

# THE AI ACT

## MARKET SURVEILLANCE

When a market surveillance authority has sufficient reason to believe that an AI system may pose a **risk**, it conducts an assessment of its compliance with the Regulation.

If the assessment reveals that the AI system does not comply with the requirements set out in the Regulation, the supervisory authority requires the operator to take corrective measures within a specified period.

These corrective measures may include:

- **bringing into compliance** the AI system;
- **withdrawal** from the market; or
- the **recall** of the system.

If the operator fails to take appropriate corrective measures within the required period, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system from being made available or put into service on the national market, to withdraw the AI system from the market, or to recall it.

# THE AI ACT

## REMEDIES

Without prejudice to other administrative or judicial remedies, any natural or legal person who has reason to believe that there has been an infringement of the provisions of the Regulation may **lodge** a reasoned **complaint** with the relevant market surveillance authority.

Any affected person who is the subject of a decision taken by the deployer on the basis of the output of a high-risk AI system listed in Annex III, with the exception of AI systems deployed in the critical infrastructure sector, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an **adverse impact on their health, safety or fundamental rights** has the right to **obtain clear and meaningful explanations from the deployer** on the role of the AI system in the decision-making procedure and on the main elements of the decision taken.

# THE AI ACT

CODES OF CONDUCT AND GUIDELINES

ADVANT Nctm



# THE AI ACT

## CODES OF CONDUCT

The AI Office and the Member States promote and facilitate the development of **voluntary codes of conduct** in relation to AI systems other than high-risk systems, in order to apply to these systems some or all of the requirements specified for high-risk AI systems.

Codes of conduct may include **clear objectives** and **key performance indicators** including:

- compliance with the Union's ethical guidelines for trustworthy AI;
- reducing the environmental impact of AI systems;
- promotion of AI literacy;
- inclusive and diverse design of AI systems;
- assessing and preventing the negative impact of AI systems on vulnerable persons or group.

Codes of conduct can be developed by individual **providers, deployers or representative organisations**, involving deployers and other stakeholders, such as SMEs, start-ups, civil society and academia.

# THE AI ACT

## GUIDELINES

The Commission draws up practical **guidelines** for the implementation of the Regulation in relation to aspects such as:

- application of the requirements and obligations laid down in the Regulation;
- prohibited practices;
- implementation of the substantive amendment provisions;
- practical implementation of transparency obligations;
- relationship between the Regulation and other EU legislation;
- application of the definition of AI system.

The Commission **updates** the guidelines at the request of the Member States, the AI Office or on its own initiative when it considers it necessary.

# THE AI ACT

DELEGATION OF POWER AND  
COMMITTEE PROCEDURE



# THE AI ACT

## DELEGATION OF POWER AND COMMITTEE PROCEDURE

The Regulation empowers the Commission to adopt **delegated acts** in relation to specific aspects identified by the Regulation.

The delegation has a duration of **5 years** (tacitly renewable) from the date of entry into force of the Regulation and may be revoked at any time by the European Parliament and the Council.

The Commission:

- before the adoption of a delegated act, **consult** the experts designated by each Member State;
- at the same time as the adoption, it **shall notify** the European Parliament and the Council of the adopted delegated act.

If the European Parliament and the Council do not object within three months of notification or if they inform the Commission that they will not object, the delegated act shall enter into force.

In its regulatory legislative work, the Commission makes use of the committee procedure. This is a mechanism that allows Member States to be involved in the preparation of delegated acts to the Commission.

# THE AI ACT

## SANCTIONS

ADVANT Nctm



# THE AI ACT

## NATURE AND EXTENT OF SANCTIONS

It is up to the Member States to lay down the rules on sanctions and other enforcement measures.

These may include, according to the Regulation:

- simple **warnings**; or
- **administrative fines**.

Sanctions must be effective, proportionate and dissuasive and take into account the economic viability of SMEs, including start-ups.

They are imposed by national market surveillance authorities.

The regulation sets the legal maximum of the applicable administrative fines, distinguishing according to whether the violation was committed by:

- AI system **operators** (i.e. providers, authorised representatives, importers, distributors and deployers);
- providers and authorised representatives of **general-purpose models**;
- **institutions and bodies of the Union**.

# THE AI ACT

## AI SYSTEMS OPERATORS

Entities	Violations
Up to <b>€35 million</b> or <b>7%</b> of total worldwide annual turnover for the previous year, if higher, if the offender is a company	Placing on the market or putting into service of prohibited AI systems
Up to <b>€15 million</b> or <b>3%</b> of total worldwide annual turnover for the previous year, if higher, if the offender is a company	Violation of obligations relating to high-risk AI systems and of transparency obligations relating to low-risk IA systems
Up to <b>€7.5 million</b> or <b>1%</b> of total worldwide annual turnover for the previous year, if higher, if the offender is a company	Provision of incorrect, incomplete or misleading information to notified bodies or competent national authorities

# THE AI ACT

## PROVIDERS OF GENERAL-PURPOSES AI MODELS

Entities	Violations
Up to <b>€15 million</b> or <b>3%</b> of total annual worldwide turnover for the previous year, if higher, , if the offender is a company	Violations of general-purpose AI model provisions

# THE AI ACT

UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

Entities	Violations
Up to <b>€1.5 million</b>	Placing on the market or putting into service of prohibited AI systems
Up to <b>€750,000</b>	Infringement of other obligations

# THE AI ACT

## CRITERIA FOR DETERMINING THE AMOUNT OF THE ADMINISTRATIVE FINES

In determining the amount of the administrative fine, account shall be taken of:

- the **nature, gravity** and **duration of** the infringement and its consequences;
- **previous sanctions** applied by other supervisory authorities against the same operator in relation to the same infringement;
- **previous sanctions** imposed for infringements of other EU legislation for infringements arising from the same activity/omission;
- the **size**, annual **turnover** and **market share** of the operator;
- other **aggravating** or **mitigating** factors (e.g. financial benefits achieved or losses avoided);
- the degree of **cooperation** with the supervisory authority;
- the degree of **responsibility** of the operator, taking into account the technical and organisational measures implemented;
- the manner in which the authority became **aware** of the infringement;
- the **intentional or negligent** character of the infringement;
- **actions taken** to mitigate the harm.

# ADVANT MEMBER FIRM OFFICES

## BEIJING

Suite 3130, 31st Floor  
South Office Tower  
Beijing Kerry Centre  
1 Guang Hua Road  
Chao Yang District  
100020 Beijing, China  
beijing@advant-beiten.com  
T: +86 10 85298110

## BERLIN

Lützowplatz 10  
10785 Berlin, Germany  
berlin@advant-beiten.com  
T: +49 30 26471-0

## BRUSSELS

Avenue Louise 489  
1050 Brussels, Belgium  
brussels@advant-beiten.com  
T: +32 2 6390000

## DUSSELDORF

Cecilienallee 7  
40474 Dusseldorf, Germany  
dusseldorf@advant-beiten.com  
T: +49 211 518989-0

## FRANKFURT

Mainzer Landstrasse 36  
60325 Frankfurt/Main, Germany  
frankfurt@advant-beiten.com  
T: +49 69 756095-0

## FREIBURG

Heinrich-von-Stephan-Strasse 25  
79100 Freiburg im Breisgau, Germany  
freiburg@advant-beiten.com  
T: +49 761 150984-0

## GENOA

Via Roma 10  
16121 Genoa, Italy  
genoa@advant-nctm.com  
T: +39 010 8531407

## HAMBURG

Neuer Wall 72  
20354 Hamburg, Germany  
hamburg@advant-beiten.com  
T: +49 40 688745-0

## LONDON

40 Bruton Street  
London, W1J 6QZ, United Kingdom  
london@advant-nctm.com  
T: +44 20 73759900

## MILAN

Via Agnello 12  
20121 Milan, Italy  
milan@advant-nctm.com  
T: +39 02 725 511

## MOSCOW

Turchaninov Per. 6/2  
119034 Moscow, Russia  
moscow@advant-beiten.com  
T: +7 495 2329635

## MUNICH

Ganghoferstrasse 33  
80339 Munich, Germany  
munich@advant-beiten.com  
T: +49 89 35065-0

## PARIS

45 Rue de Tocqueville  
75017 Paris, France  
paris@advant-altana.com  
T: +33 1 79 97 93 00

## ROME

Via delle Quattro Fontane 161  
00187 Rome, Italy  
rome@advant-nctm.com  
T: +39 06 6784977

## SHANGHAI

Room 4102  
Hong Kong New World Tower  
No. 300 Middle Huaihai Road  
200032 Shanghai Shi, China  
shanghai@advant-nctm.com  
T: +86 21 60906337