REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

EU Artificial Intelligence Act Purpose

Establish:

- Harmonized rules for the placing on the market, the putting into service and the use of artificial intelligence systems (‘AI systems’) in the Union
- Prohibitions of certain artificial intelligence practices
- Specific requirements for high-risk AI systems and obligations for operators of such systems
- Harmonized transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorization systems, and AI systems used to generate or manipulate image, audio or video content
- Rules on market monitoring and surveillance

EU Artificial Intelligence Act Scope

- Providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country
- Users of AI systems located within the Union
- Providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union
- Not apply to AI systems developed or used exclusively for military purposes
- Not apply to public authorities in a third country nor to international organizations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organizations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States

EU Artificial Intelligence Act
Some Key Definitions

- **'artificial intelligence system' (AI system)**: Software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with
- **'provider'**: A natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge
- **'user'**: Any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity
- **'authorized representative'**: Any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation
- **'importer'**: Any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union
- **'distributor'**: Any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties

EU Artificial Intelligence Act
Some Key Definitions

- **'notifying authority'**: The national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring
- **'conformity assessment'**: The process of verifying whether the requirements set out in the EU AI Act relating to an AI system have been fulfilled
- **'conformity assessment body'**: A body that performs third-party conformity assessment activities, including testing, certification and inspection
- **'notified body'**: A conformity assessment body designated in accordance with this Regulation and other relevant Union harmonization legislation
- **'national supervisory authority'**: The authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board
- **'national competent authority'**: The national supervisory authority, the notifying authority and the market surveillance authority

EU Artificial Intelligence Act Prohibited Practices

- The placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm
- The placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm
- The placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behavior or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:
  - Detrimental or unfavorable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
  - Detrimental or unfavorable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity
-

EU Artificial Intelligence Act Prohibited Practices

- The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:
  - the targeted search for specific potential victims of crime, including missing children
  - the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack
  - the detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State
- The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:
  - the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system
  - the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system

EU Artificial Intelligence Act
Hi-Risk AI Systems

A Hi-Risk AI System meets both of the following conditions:

- The AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonization legislation listed in Annex I
- The product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonization legislation listed in Annex II

AI Systems can be added to the list of Hi-Risk AI Systems if thry meet both of the following conditions:

- The AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III
- The AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III

EU Artificial Intelligence Act
Hi-Risk AI Systems

The following are categories of Hi-Risk AI Systems

- Biometric identification and categorization of natural persons:
  - AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons
- Management and operation of critical infrastructure
  - AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity
- Education and vocational training:
  - AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions
  - AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions

1. Employment, workers management and access to self-employment:
   - AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests
   - AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships

EU Artificial Intelligence Act
Hi-Risk AI Systems

The following are categories of Hi-Risk AI Systems

- Access to and enjoyment of essential private services and public services and benefits:
  - AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services
  - AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use
  - AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid
- Law enforcement:
  - (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences
  - (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person
  - (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in this regulation
  - (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences

EU Artificial Intelligence Act
Hi-Risk AI Systems

The following are categories of Hi-Risk AI Systems

- Law enforcement (cont):
  - AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups
  - AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences
  - AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data
- Administration of justice and democratic processes:
  - AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts

EU Artificial Intelligence Act Risk Management System

- Shall be established, implemented, documented and maintained in relation to high-risk AI systems
- Shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating
- Shall comprise the following:
  - Identification and analysis of the known and foreseeable risks associated with each high-risk AI system
  - Estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse
  - Evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system
  - Adoption of suitable risk management measures
- Specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children

EU Artificial Intelligence Act Risk Management System

In identifying the most appropriate risk management measures, the following shall be ensured:

- Elimination or reduction of risks as far as possible through adequate design and development
- Where appropriate, implementation of adequate mitigation and control
- Measures in relation to risks that cannot be eliminated
- Measures shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:
  - Fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible
  - Remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons
  - Be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available
  - Be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system
  - Be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure

EU Artificial Intelligence Act
Hi-Risk AI Systems Testing

- High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures.
- Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements
- Testing procedures shall be suitable to achieve the intended purpose of the AI system and do not need to go beyond what is necessary to achieve that purpose
- The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service
- Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system

EU Artificial Intelligence Act
Hi-Risk AI Systems Requirements

High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria:

- Training, validation and testing data sets shall be subject to appropriate data governance and management practices
- Training, validation and testing data sets shall be relevant, representative, free of errors and complete
- Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioral or functional setting within which the high risk AI system is intended to be used
- Appropriate data governance and management practices shall apply for the development of high-risk AI systems

EU Artificial Intelligence Act
Other Hi-Risk AI Systems Requirements

Technical documentation of a high-risk AI system shall

- Be drawn up before that system is placed on the market or put into service and shall be kept up-to date
- Provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with its requirements

Record Keeping shall:

- Be designed and developed with capabilities enabling the automatic recording of events (‘logs’) while the high-risk AI systems is operating
- Logging capabilities shall ensure a level of traceability of the AI system’s functioning throughout its lifecycle that is appropriate to the intended purpose of the system
- Logging capabilities shall provide, at a minimum:
  - Recording of the period of each use of the system (start date and time and end date and time of each use)
  - The reference database against which input data has been checked by the system
  - Input data for which the search has led to a match
  - Identification of the natural persons involved in the verification of the results

EU Artificial Intelligence Act
Other Hi-Risk AI Systems Requirements

- High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately
- High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use
2. Human oversight shall aim at preventing or minimizing the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse
3. Human oversight shall be ensured through either one or all of the following measures:
    - Identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service
    - Identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user

EU Artificial Intelligence Act
Other Hi-Risk AI Systems Requirements

- High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle
- The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use
- High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems
- High-risk AI systems shall be resilient as regards attempts by unauthorized third parties to alter their use or performance by exploiting the system vulnerabilities

EU Artificial Intelligence Act
Requirements on Hi-Risk AI Systems Providers

Providers of high-risk AI systems shall:

- Ensure that their high-risk AI systems are compliant with Hi-Risk AI Systems requirements
- Have a quality management system in place which complies with the AI Act
- Provide the technical documentation of the high-risk AI system
- When under their control, keep the logs automatically generated by their high-risk AI systems
- Ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service
- Comply with the registration obligations
- Take the necessary corrective actions, if the high-risk AI system is not in conformity with requirements
- Inform the appropriate national competent authorities of any corrective actions taken
- Affix the marking to their high-risk AI systems to indicate the conformity with the AI Act
- Upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with requirements

EU Artificial Intelligence Act
Requirements on Hi-Risk AI Systems Providers

Providers of high-risk AI systems shall:

- Put a quality management system in place that ensures compliance with this Regulation
- That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions
- Implementation of written policies, procedures and instructions shall be proportionate to the size of the provider's organization
- Draw up the technical documentation that meets the requirements of the AI Act
- Ensure that their systems undergo the relevant conformity assessment procedure in accordance with the AI Act prior to their placing on the market or putting into service
- Keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law
- Logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law
- Immediately take the necessary corrective actions if non-conformities are found to bring that system into conformity, to withdraw it or to recall it, as appropriate
- Inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly

EU Artificial Intelligence Act
Requirements on Hi-Risk AI Systems Providers

Providers of high-risk AI systems shall:

- Upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements of the AI Act
- Where the high-risk AI system presents a risk and that risk is known to the provider of the system, immediately inform the national competent authorities of the Member States in which it made the system available and, where applicable, the notified body that issued a certificate for the high-risk AI system of the non-compliance and of any corrective actions taken

EU Artificial Intelligence Act
Requirements on Hi-Risk AI Systems Users

Users of high-risk AI systems shall:

- Use such systems in accordance with the instructions of use accompanying the systems
- To the extent the user exercises control over the input data, ensure that input data is relevant in view of the intended purpose of the high-risk AI system
- Monitor the operation of the high-risk AI system on the basis of the instructions of use
- When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of AI Act, inform the provider or distributor and suspend the use of the system
- Inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of the AI Act and interrupt the use of the AI system
- Keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control
- Use the information provided under the AI Act to comply with their obligation to carry out a data protection impact assessment

EU Artificial Intelligence Act Transparency Requirements for Hi-Risk AI Systems

- Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use
- Users of an emotion recognition system or a biometric categorization system shall inform of the operation of the system the natural persons exposed thereto
  - Does not apply to AI systems used for biometric categorization which are permitted by law to detect, prevent and investigate criminal offences
- Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated
  - However, does not apply where the use is authorized by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties

EU Artificial Intelligence Act
Other Chapters

The AI Act has chapters that deal with topics such as:

- Requirements for product manufacturers, authorized representatives, importers third parties and distributers of Hi-Risk AI Systems
- Requirements pertaining to notification of National Bodies and Notifying Authorities
- Conformity Assessments and issuance of Conformity Certificates
- Processing of personal data
- Development, testing and validation of innovative AI systems
- Establishment of the European Artificial Intelligence Board
- Establishment of national competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of the AI Act
- Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems
- Reporting of serious incidents and of malfunctioning
- Procedure for dealing with AI systems presenting a risk at national level