Brussels, 14.11.2022 COM (2022)

2022/001 (MEUC)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT)

Edited for the Model European Union Conference

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee,

Having regard to the opinion of the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

(2) Artificial intelligence systems (AI systems) can be easily deployed in multiple sectors of the economy and society, including cross border, and circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations. Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI systems. A consistent and high level of protection throughout the Union should

therefore be ensured, while divergences hampering the free circulation of AI systems and related products and services within the internal market should be prevented, by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

(3) A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. By laying down those rules, this Regulation supports the objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence, as stated by the European Council[1], and it ensures the protection of ethical principles, as specifically requested by the European Parliament[2].

(4) The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension. AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded). The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to–date in the light of market and technological developments through the adoption of delegated acts by the Commission to amend that list.

HAVE ADOPTED THIS REGULATION:

---

1 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

2 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

TITLE I

GENERAL PROVISIONS

ARTICLE 1
SUBJECT MATTER

This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;

(b) prohibitions of certain artificial intelligence practices;

(c) specific requirements for high-risk AI systems and obligations for operators of such systems;

(d) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;

(e) rules on market monitoring and surveillance.

ARTICLE 2
SCOPE

1. This Regulation applies to:

(a) 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;

(b) users of AI systems located within the Union;

(c) 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.

2. This Regulation shall not apply to AI systems developed or used exclusively for military purposes.

ARTICLE 3
DEFINITIONS

For the purpose of this Regulation, the following definitions apply:

(1) 'artificial intelligence system' (AI system) is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human based data and inputs to:

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods;

(2) 'provider' means 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;

(3) 'user' means 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;

(4) 'authorised representative' means 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;

(5) 'importer' means 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;

(6) 'distributor' means 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;

(7) 'operator' means the provider, the user, the authorised representative, the importer and the distributor.

ARTICLE 4

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

The following artificial intelligence practices shall be prohibited:

(a) 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 behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(b) 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 in accordance with the characteristics as outlined in Article 21 of the Charter of the Fundamental Rights of the European Union, 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;

(c) 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 behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable 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;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) unless and in as far as such use is necessary, as determined by the Member States, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement.

TITLE II

HIGH-RISK AI SYSTEMS

CHAPTER 1

CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

ARTICLE 5

CLASSIFICATION RULES FOR HIGH-RISK AI SYSTEMS

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

   (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation;

   (b) 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 harmonisation.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

CHAPTER 2

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

ARTICLE 6

COMPLIANCE WITH THE REQUIREMENTS

1. High-risk AI systems shall comply with the requirements established in this Chapter.

2. The intended purpose of the high-risk AI system and the risk management system referred to in Article 7 shall be taken into account when ensuring compliance with those requirements.

ARTICLE 7

RISK MANAGEMENT SYSTEM

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

2. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:

   (a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

   (b) 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;

   (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system;

   (d) 'regular' is to be defined as 'every 18 Months';

   (e) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.

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

   (a) elimination or reduction of risks as far as possible through adequate design and development;

   (b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated.

4. 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 set out in this Chapter.

5. 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.

6. When implementing the risk management system described in paragraphs 1 to 5, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children and young adults.

7. AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment, testing that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan; this shall take place under the direct supervision and guidance by the competent authorities with a view to ensuring compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation supervised within the sandbox.

Article 8
Data and data governance

1. 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 referred to in paragraphs 2 to 4.

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular:

   (a) the relevant design choices;

   (b) data collection;

   (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;

   (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;

   (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;

   (f) examination in view of possible biases;

   (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.

4. 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, behavioural or functional setting within which the high-risk AI system is intended to be used.

Article 9
Technical documentation

The 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.

Article 10
Record-keeping

1. High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events (‘logs’) while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications, preferably established in the Union, including but not limited to: Regulations 2016/679 (GDPR) of the European Parliament and of the Council.

2. The 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.

3. For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum:

   (a) recording of the period of each use of the system (start date and time and end date and time of each use);

   (b) the reference database against which input data has been checked by the system;

   (c) the input data for which the search has led to a match;

   (d) the identification of the natural persons involved in the verification of the results.

Article 11

Transparency and provision of information to users

1. 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. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title.

2. 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.

Article 12

Human oversight

1. High-risk AI systems must 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 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, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.

3. Human oversight must be ensured through either one or all of the following measures:

   (a) identified and built into the high-risk AI system by the provider before it is placed on the market or put into service;

   (b) 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.

4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

   (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation;

(b) 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;

(c) 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;

(d) be able to intervene in the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

5. If human oversight is not possible under the circumstances listed above, the high-risk AI system must not enter the common market.

Article 13

Accuracy, robustness and cybersecurity

1. 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.

2. 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.

   The robustness of high-risk AI systems must be achieved through technical redundancy solutions. They must include backup or fail-safe plans.

Chapter 3

OBLIGATIONS OF PROVIDERS AND USERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES

Article 14

Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;

(b) draw-up the technical documentation of the high-risk AI system;

(c) when under their control, keep the logs automatically generated by their high-risk AI systems;

(d) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

(e) take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;

(f) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;

(g) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

Article 15
Automatically generated logs

Providers of high-risk AI systems shall 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. The logs shall be kept for at least 5 years.

Article 16
Cooperation with competent authorities

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 set out in Chapter 2 of this Title, in an official Union language determined by the Member State concerned. Upon a reasoned request from a national competent authority, providers shall also give that authority access to the logs automatically generated by the high-risk AI system, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law.

Article 17
Obligations of users of high-risk AI systems

1. Users of high-risk AI systems shall use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 3.

2. The obligations in paragraph 1 are without prejudice to other user obligations under Union or national law and to the user's discretion in organizing its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

3. Without prejudice to paragraph 1, to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.

TITLE III

GOVERNANCE

CHAPTER 1

EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

ARTICLE 18
ESTABLISHMENT OF THE EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

1. A 'European Artificial Intelligence Board' (the 'Board') is established.
2. The Board shall provide advice and assistance to the Commission in order to:
   (a) contribute to the effective cooperation of the national supervisory authorities and the Commission with regard to matters covered by this Regulation;
   (b) coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation;
   (c) assist the national supervisory authorities and the Commission in ensuring the consistent application of this Regulation.
3. The board shall have its headquarters in Berlin, Germany.

ARTICLE 19
STRUCTURE OF THE BOARD

1. The Board shall be composed of the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them.
2. The Board shall adopt its rules of procedure by a simple majority of its members, following the consent of the Commission. The rules of procedure shall also contain the operational aspects related to the execution of the Board's tasks as listed in Article 20. The Board may establish sub-groups as appropriate for the purpose of examining specific questions.
3. The Board shall be chaired by the Commission. The Commission shall convene the meetings and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and with its rules of procedure. The Commission shall provide administrative and analytical support for the activities of the Board pursuant to this Regulation.

ARTICLE 20
TASKS OF THE BOARD

When providing advice and assistance to the Commission in the context of Article 18(2), the Board shall in particular:

(a) collect and share opinions, expertise and best practices among Member States in particular but not limited to those from civil society, interest groups and AI providers;

(b) issue opinions, recommendations or written contributions on matters related to the implementation of this Regulation, in particular:

(i) on technical specifications or existing standards regarding the requirements set out in Title II, Chapter 2,

(ii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 25.

Article 21

EU database for stand-alone high-risk AI systems

1. The Commission shall, in collaboration with the Member States, set up and maintain an EU database containing information concerning high-risk AI systems.

2. Information contained in the EU database shall be accessible to the public.

3. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation.

4. The board shall be the controller of the EU database. It shall also ensure to providers adequate technical and administrative support.

TITLE IV

Enforcement

Article 22

Market surveillance and control of AI systems in the Union market

1. Member States shall designate a market surveillance authority and shall report to the Commission on a regular basis the outcomes of relevant market surveillance activities. They shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules.

2. For AI systems placed on the market, put into service or used by financial institutions regulated by Union legislation on financial services, the market surveillance authority shall be the European Central Bank (ECB).

Article 23

Access to data and documentation

1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming

interfaces ('API') or other appropriate technical means and tools enabling remote access.

2. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights in relation to the use of high-risk AI systems shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.

3. One month after the entering into force of this Regulation, each Member State shall identify the public authorities or bodies referred to in paragraph 2 and make a list publicly available on the website of the national supervisory authority. Member States shall notify the list to the Commission and all other Member States and keep the list up to date.

Article 23a
European Database

A European database of non-biased data is put in place. It is available to all research institutions and businesses which develop AI and is to be used for research purposes only. It only contains non-personal data in order to prevent discrimination.

Article 24
Procedure for dealing with AI systems presenting a risk at national level

1. AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned.

2. Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, they shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to the protection of fundamental rights are present, the market surveillance authority shall also inform the relevant national public authorities or bodies. The relevant operators shall cooperate as necessary with the market surveillance authorities.

   Where, in the course of that evaluation, the market surveillance authority finds that the AI system does not comply with the requirements and obligations laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

3. The operator shall ensure that all appropriate corrective action is taken in respect of all the AI systems concerned that it has made available on the market throughout the Union.

4. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market, to withdraw the product from that market or to

recall it. That authority shall inform the Commission and the other Member States, without delay, of those measures.

5. The information shall include all available details, in particular the data necessary for the identification of the non-compliant AI system, the origin of the AI system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator.

6. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the AI system concerned, and, in the event of disagreement with the notified national measure, of their objections.

7. Where, within three months of receipt of the information referred to in paragraph 4, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020.

8. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product concerned, such as withdrawal of the product from their market, without delay.

TITLE V

PENALTIES

ARTICLE 25
PENALTIES

1. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, including administrative fines, applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into particular account the interests of small-scale providers and start-up and their economic viability.

2. The Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

3. The following infringements shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is company, up to 5% of its total worldwide annual turnover for the preceding financial year, whichever is higher:

   (a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 4;

   (b) non-compliance of the AI system with the requirements laid down in Article 8.

4. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 4 and 8, shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The intentional, repeated or negligent supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 12% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement and of its consequences;

   (b) whether administrative fines have been already applied by other market surveillance authorities to the same operator for the same infringement;

   (c) the size and market share of the operator committing the infringement.

Article 26

Administrative fines on Union institutions, agencies and bodies

1. The European Data Protection Supervisor may impose administrative fines on Union institutions, agencies and bodies falling within the scope of this Regulation.

2. The following infringements shall be subject to administrative fines of up to 1 000 000 EUR:

   (a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 4;

   (b) non-compliance of the AI system with the requirements laid down in Article 8.

3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 4 and 8, shall be subject to administrative fines of up to 500 000 EUR.

4. Funds collected by imposition of fines in this Article shall be the income of the general budget of the Union.

TITLE VI

Final Provision

Article 27

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply 18 months from the AI Act's entry into force.

This Regulation shall be binding in its entirety and applicable in all Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 5(2)

High-risk AI systems pursuant to Article 5(2) are the AI systems listed in any of the following areas:

1. Biometric identification and categorisation of natural persons:
   (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;
2. Management and operation of critical infrastructure:
   (a) 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.
3. Education and vocational training:
   (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
   (b) 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.
4. Employment, workers management and access to self-employment:
   (a) 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;
   (b) 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.
5. Access to and enjoyment of essential private services and public services and benefits:
   (a) 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;
   (b) 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;
   (c) 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.
6. 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 for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(d) 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;

(e) 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;

(f) 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.

7. Migration, asylum and border control management:

(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

(d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:

(a) 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.