EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

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

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

2021/0106 (COD)

Proposal for a

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

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[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

HAVE ADOPTED THIS REGULATION:

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;

(a) prohibitions of certain artificial intelligence practices;

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

(c) 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;

(d) rules on market monitoring and surveillance.

[1] OJ C […], […], p. […].
[2] OJ C […], […], p. […].

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;

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

4. This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations 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.

5. This Regulation shall not affect the application of the provisions on the liability of intermediary service providers set out in Chapter II, Section IV of Directive 2000/31/EC of the European Parliament and of the Council[3] [*as to be replaced by the corresponding provisions of the Digital Services Act*].

Article 3
Definitions

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

(1) 'artificial intelligence system' (AI system) means 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;

(1) '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) 'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC[4];

(4) '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;

(5) '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,

---

[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

[4] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;

(6) ‘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;

(7) ‘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;

(8) ‘operator’ means the provider, the user, the authorised representative, the importer and the distributor;

(9) ‘placing on the market’ means the first making available of an AI system on the Union market;

(10) ‘making available on the market’ means any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(11) ‘putting into service’ means the supply of an AI system for first use directly to the user or for own use on the Union market for its intended purpose;

(12) ‘intended purpose’ means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(13) ‘reasonably foreseeable misuse’ means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;

(14) ‘safety component of a product or system’ means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property;

(15) ‘instructions for use’ means the information provided by the provider to inform the user of in particular an AI system’s intended purpose and proper use, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used;

(16) ‘recall of an AI system’ means any measure aimed at achieving the return to the provider of an AI system made available to users;

(17) ‘withdrawal of an AI system’ means any measure aimed at preventing the distribution, display and offer of an AI system;

(18) ‘performance of an AI system’ means the ability of an AI system to achieve its intended purpose;

(19) ‘notifying authority’ means 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;

(20) ‘conformity assessment’ means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled;

(21) ‘conformity assessment body’ means a body that performs third-party conformity assessment activities, including testing, certification and inspection;

(22) ‘notified body’ means a conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation;

(23) ‘substantial modification’ means a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation or results in a modification to the intended purpose for which the AI system has been assessed;

(24) ‘CE marking of conformity’ (CE marking) means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 of this Regulation and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;

(25) ‘post-market monitoring’ means all activities carried out by providers of AI systems to proactively collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

(26) ‘market surveillance authority’ means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020;

(27) ‘harmonised standard’ means a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012;

(28) ‘common specifications’ means a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under this Regulation;

(29) ‘training data’ means data used for training an AI system through fitting its learnable parameters, including the weights of a neural network;

(30) ‘validation data’ means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split;

(31) ‘testing data’ means data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service;

(32) ‘input data’ means data provided to or directly acquired by an AI system on the basis of which the system produces an output;

(33) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(34) ‘emotion recognition system’ means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(35) ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour,

tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;

(36) ‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

(37) ‘‘real-time’ remote biometric identification system’ means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.

(38) ‘‘post’ remote biometric identification system’ means a remote biometric identification system other than a ‘real-time’ remote biometric identification system;

(39) ‘publicly accessible space’ means any physical place accessible to the public, regardless of whether certain conditions for access may apply;

(40) ‘law enforcement authority’ means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(41) ‘law enforcement’ means activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(42) ‘national supervisory authority’ means 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;

(43) ‘national competent authority’ means the national supervisory authority, the notifying authority and the market surveillance authority;

(44) ‘serious incident’ means any incident that directly or indirectly leads, might have led or might lead to any of the following:

(a) the death of a person or serious damage to a person’s health, to property or the environment,

(b) a serious and irreversible disruption of the management and operation of critical infrastructure.

Article 4
Amendments to Annex I

The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.

TITLE II

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Article 5

1. 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 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;

   (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) 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:

      (i) the targeted search for specific potential victims of crime, including missing children;

      (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

2. 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:

(a) 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;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, 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 comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

TITLE III

HIGH-RISK AI SYSTEMS

CHAPTER 1

CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

Article 6
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 listed in Annex II;

(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 legislation listed in Annex II.

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.

Article 7
Amendments to Annex III

1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

   (a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;

   (b) 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.

2. When assessing for the purposes of paragraph 1 whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights that is equivalent to or greater than the risk of harm posed by the high-risk AI systems already referred to in Annex III, the Commission shall take into account the following criteria:

   (a) the intended purpose of the AI system;

   (b) the extent to which an AI system has been used or is likely to be used;

   (c) the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities;

   (d) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;

   (e) the extent to which potentially harmed or adversely impacted persons are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

   (f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;

   (g) the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;

   (h) the extent to which existing Union legislation provides for:

      (i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

      (ii) effective measures to prevent or substantially minimise those risks.

CHAPTER 2

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Article 8
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 9 shall be taken into account when ensuring compliance with those requirements.

Article 9
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 referred to in Article 61;

   (d) 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;

   (c) provision of adequate information pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

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.

Article 10
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 5.

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.

5. It is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data subject to appropriate safeguards for the fundamental rights and freedoms of natural persons.

Article 11
Technical documentation

1. 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.

   The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV.

Article 12
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.

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, as referred to in Article 14 (5).

Article 13
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.

3. The information referred to in paragraph 2 shall specify:

   (a) the identity and the contact details of the provider and, where applicable, of its authorised representative;

   (b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

      (i) its intended purpose;

      (ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

      (iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights;

(iv) its performance as regards the persons or groups of persons on which the system is intended to be used;

(v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system.

(c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;

(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;

(e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates.

Article 14
Human oversight

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 minimising 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 shall be ensured through either one or all of the following measures:

(a) 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;

(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, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

(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 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;

(e) 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.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.

Article 15
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. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

3. 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 may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures.

4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

CHAPTER 3

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

Article 16
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) have a quality management system in place which complies with Article 17;

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

(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) comply with the registration obligations referred to in Article 51;

Article 17
Quality management system

1. 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, and shall include at least the following aspects:

   (a) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;

   (b) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;

   (c) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;

   (d) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;

   (e) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;

   (f) systems and procedures for record keeping of all relevant documentation and information;

   (g) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.

2. The implementation of aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation.

Article 18
Obligation to draw up technical documentation

1. Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.

Article 19
Conformity assessment

1. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following

that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.

Article 20
Automatically generated logs

1. 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 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.

Article 21
Corrective actions

Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly.

Article 22
Duty of information

Where the high-risk AI system presents a risk within the meaning of Article 65(1) and that risk is known to the provider of the system, that provider shall 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, in particular of the non-compliance and of any corrective actions taken.

Article 23
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 24
Obligations of product manufacturers

Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance

of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider.

Article 25
Authorised representatives

1. Prior to making their systems available on the Union market, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union.

2. The authorised representative shall perform the tasks specified in the mandate received from the provider.

Article 26
Obligations of importers

1. Before placing a high-risk AI system on the market, importers of such system shall ensure that:

   (a) the appropriate conformity assessment procedure has been carried out by the provider of that AI system

   (b) the provider has drawn up the technical documentation

   (c) the system bears the required conformity marking and is accompanied by the required documentation and instructions of use.

2. Where an importer considers or has reason to consider that a high-risk AI system is not in conformity with this Regulation, it shall not place that system on the market until that AI system has been brought into conformity.

3. Importers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable.

4. Importers shall ensure that the high-risk AI system they are importing is under their responsibility.

Article 27
Obligations of distributors

1. Before making a high-risk AI system available on the market, distributors shall verify that the high-risk AI system bears the required CE conformity marking, that it is accompanied by the required documentation and instruction of use, and that the provider and the importer of the system, as applicable, have complied with the obligations set out in this Regulation.

2. Upon a reasoned request from a national competent authority, distributors of high-risk AI systems shall provide that authority with all the information and documentation necessary to demonstrate the conformity of a high-risk system with the requirements set out in Chapter 2 of this Title. Distributors shall also cooperate with that national competent authority on any action taken by that authority.

Article 28

Obligations of distributors, importers, users or any other third-party

1. Any distributor, importer, user or other third-party shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

   (a) they place on the market or put into service a high-risk AI system under their name or trademark;

   (b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;

   (c) they make a substantial modification to the high-risk AI system.

Article 29

Obligations of users of high-risk AI systems

1. Users shall 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 Article 65(1) they shall inform the provider or distributor and suspend the use of the system.

2. Users of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law.

CHAPTER 4

NOTIFIYING AUTHORITIES AND NOTIFIED BODIES

Article 30

Notifying authorities

1. Each Member State shall designate or establish a notifying 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.

2. Notifying authorities shall be organised in such a way that decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies.

Article 31

Application of a conformity assessment body for notification

1. Conformity assessment bodies shall submit an application for notification to the notifying authority of the Member State in which they are established.

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body

fulfils the requirements laid down in Article 33. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 33. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those designations may be used to support their designation procedure under this Regulation, as appropriate.

Article 32
Notification procedure

1. Notifying authorities shall notify the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

2. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies concerned.

3. Notifying authorities shall notify the Commission and the other Member States of any subsequent relevant changes to the notification.

Article 33
Notified bodies

1. Notified bodies shall verify the conformity of high-risk AI system in accordance with the conformity assessment procedures referred to in Article 43.

2. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks.

3. The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall be such as to ensure that there is confidence in the performance by and in the results of the conformity assessment activities that the notified bodies conduct.

4. Notified bodies shall be independent of the provider of a high-risk AI system in relation to which it performs conformity assessment activities. Notified bodies shall also be independent of any other operator having an economic interest in the high-risk AI system that is assessed, as well as of any competitors of the provider.

5. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.

6. Notified bodies shall have documented procedures in place.

7. Notified bodies shall have procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the AI system in question.

8. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State concerned in accordance with national law or that Member State is directly responsible for the conformity assessment.

9. Notified bodies shall be capable of carrying out all the tasks falling to them under this Regulation with the highest degree of professional integrity and the requisite competence in the specific field, whether those tasks are carried out by notified bodies themselves or on their behalf and under their responsibility.

10. Notified bodies shall have sufficient internal competences to be able to effectively evaluate the tasks conducted by external parties on their behalf. To that end, at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, the notified body shall have permanent availability of sufficient administrative, technical and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies, data and data computing and to the requirements set out in Chapter 2 of this Title.

11. Notified bodies shall participate in coordination activities as referred to in Article 38. They shall also take part directly or be represented in European standardisation organisations, or ensure that they are aware and up to date in respect of relevant standards.

12. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 30 to allow it to conduct its assessment, designation, notification, monitoring and surveillance activities and to facilitate the assessment outlined in this Chapter.

Article 34

Subsidiaries of and subcontracting by notified bodies

1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements laid down in Article 33 and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the provider.

4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.

Article 35

Identification numbers and lists of notified bodies designated under this Regulation

1. The Commission shall assign an identification number to notified bodies. It shall assign a single number, even where a body is notified under several Union acts.

2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been assigned to them

and the activities for which they have been notified. The Commission shall ensure that the list is kept up to date.

Article 36
Changes to notifications

1. Where a notifying authority has suspicions or has been informed that a notified body no longer meets the requirements laid down in Article 33, or that it is failing to fulfil its obligations, that authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body investigation no longer meets the requirements laid down in Article 33 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure. It shall also immediately inform the Commission and the other Member States accordingly.
2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying authority shall take appropriate steps to ensure that the files of that notified body are either taken over by another notified body or kept available for the responsible notifying authorities at their request.

Article 37
Challenge to the competence of notified bodies

1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt whether a notified body complies with the requirements laid down in Article 33.
2. The Notifying authority shall provide the Commission, on request, with all relevant information relating to the notification of the notified body concerned.
3. The Commission shall ensure that all confidential information obtained in the course of its investigations pursuant to this Article is treated confidentially.
4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements laid down in Article 33, it shall adopt a reasoned decision requesting the notifying Member State to take the necessary corrective measures, including withdrawal of notification if necessary. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 38
Coordination of notified bodies

1. The Commission shall ensure that, with regard to the areas covered by this Regulation, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures of AI systems pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**
2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

Article 39
Conformity assessment bodies of third countries

Conformity assessment bodies established under the law of a third country with which the Union has concluded an agreement may be authorised to carry out the activities of notified Bodies under this Regulation.

CHAPTER 5

STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION

Article 40
Harmonised standards

High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.

Article 41
Common specifications

1. Where harmonised standards referred to in Article 40 do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

2. The Commission, when preparing the common specifications referred to in paragraph 1, shall gather the views of relevant bodies or expert groups established under relevant sectorial Union law.

3. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that are at least equivalent thereto.

Article 42
Presumption of conformity with certain requirements

1. Taking into account their intended purpose, high-risk AI systems that have been trained and tested on data concerning the specific geographical, behavioural and functional setting within which they are intended to be used shall be presumed to be in compliance with the requirement set out in Article 10(4).

2. High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[5] and the references of which have been published in the Official Journal of the European Union shall be presumed to be

[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 1).

in compliance with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

Article 43
Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:

   (a) the conformity assessment procedure based on internal control referred to in Annex VI;

   (b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

   Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

   For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

2. High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user.

   For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.

Article 44
Certificates

1. Certificates shall be valid for the period they indicate, which shall not exceed five years. On application by the provider, the validity of a certificate may be extended for further periods, each not exceeding five years, based on a re-assessment in accordance with the applicable conformity assessment procedures.

3. Where a notified body finds that an AI system no longer meets the requirements set out in Chapter 2 of this Title, it shall, taking account of the principle of proportionality, suspend or withdraw the certificate issued or impose any restrictions on it, unless compliance with those requirements is ensured by appropriate corrective

action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.

Article 45
Appeal against decisions of notified bodies

Member States shall ensure that an appeal procedure against decisions of the notified bodies is available to parties having a legitimate interest in that decision.

Article 46
Information obligations of notified bodies

1. Notified bodies shall inform the notifying authority of the following:
   (a) any Union technical documentation assessment certificates, any supplements to those certificates, quality management system approvals issued in accordance with the requirements of Annex VII;
   (b) any refusal, restriction, suspension or withdrawal of a Union technical documentation assessment certificate or a quality management system approval issued in accordance with the requirements of Annex VII;
   (c) any circumstances affecting the scope of or conditions for notification;
   (d) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;
   (e) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.
2. Each notified body shall inform the other notified bodies of:
   (a) quality management system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued;
   (b) EU technical documentation assessment certificates or any supplements thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, of the certificates and/or supplements thereto which it has issued.

Article 47
Derogation from conformity assessment procedure

1. By way of derogation from Article 43, any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period of time, while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed. The completion of those procedures shall be undertaken without undue delay.
2. The authorisation referred to in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies with the requirements of Chapter 2 of this Title. The market surveillance authority shall

inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1.

3. Where, within 15 calendar days of receipt of the information referred to in paragraph 2, no objection has been raised by either a Member State or the Commission in respect of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.

Article 48
EU declaration of conformity

1. The provider shall draw up a written EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.

2. The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into an official Union language or languages required by the Member State(s) in which the high-risk AI system is made available.

Article 49
CE marking of conformity

1. The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.

Article 50
Document retention

The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:

(a) the technical documentation referred to in Article 11;

(b) the documentation concerning the quality management system referred to Article 17;

(c) the documentation concerning the changes approved by notified bodies where applicable;

(d) the decisions and other documents issued by the notified bodies where applicable;

(e) the EU declaration of conformity referred to in Article 48.

Article 51
Registration

Before placing on the market or putting into service a high-risk AI system referred to in Article 6(2), the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.

TITLE IV

TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS

Article 52
Transparency obligations for certain AI systems

1. 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. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.

3. 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, the first subparagraph shall not apply where the use is authorised 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.

4. Paragraphs 1, 2 and 3 shall not affect the requirements and obligations set out in Title III of this Regulation.

TITLE V

MEASURES IN SUPPORT OF INNOVATION

Article 53
AI regulatory sandboxes

1. AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment 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.

2. Member States shall ensure that to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data,

the national data protection authorities and those other national authorities are associated to the operation of the AI regulatory sandbox.

3. The AI regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place.

4. Participants in the AI regulatory sandbox shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result from the experimentation taking place in the sandbox.

5. Member States' competent authorities that have established AI regulatory sandboxes shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board and they shall submit annual reports to the Board and the Commission.

Article 54

Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox

1. In the AI regulatory sandbox personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the following conditions:

   (a) the innovative AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas:

      (i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;

      (ii) public safety and public health, including disease prevention, control and treatment;

      (iii) a high level of protection and improvement of the quality of the environment;

   (b) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the participants and only authorised persons have access to that data;

   (c) any personal data processed in the context of the sandbox are deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;

   (d) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox and 1 year after its termination, solely for the purpose of and only as long as necessary for fulfilling accountability and documentation obligations under this Article or other application Union or Member States legislation;

(e) complete and detailed description of the process and rationale behind the training, testing and validation of the AI system is kept together with the testing results as part of the technical documentation in Annex IV;

(f) a short summary of the AI project developed in the sandbox, its objectives and expected results published on the website of the competent authorities.

Article 55
Measures for small-scale providers and users

1. Member States shall undertake the following actions:

(a) provide small-scale providers and start-ups with priority access to the AI regulatory sandboxes to the extent that they fulfil the eligibility conditions;

(b) organise specific awareness raising activities about the application of this Regulation tailored to the needs of the small-scale providers and users;

(c) where appropriate, establish a dedicated channel for communication with small-scale providers and user and other innovators to provide guidance and respond to queries about the implementation of this Regulation.

2. The specific interests and needs of the small-scale providers shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size and market size.

TITLE VI

GOVERNANCE

CHAPTER 1

EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

Article 56
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.

Article 57
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.

Article 58
Tasks of the Board

When providing advice and assistance to the Commission in the context of Article 56(2), the Board shall in particular:

(a) collect and share expertise and best practices among Member States;

(b) contribute to uniform administrative practices in the Member States, including for the functioning of regulatory sandboxes referred to in Article 53;

(c) 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 III, Chapter 2,

  (ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,

  (iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71.

CHAPTER 2

NATIONAL COMPETENT AUTHORITIES

Article 59
Designation of national competent authorities

1. National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks.

2. Each Member State shall designate a national supervisory authority among the national competent authorities. The national supervisory authority shall act as notifying authority and market surveillance authority unless a Member State has organisational and administrative reasons to designate more than one authority.

3. Member States shall inform the Commission of their designation or designations and, where applicable, the reasons for designating more than one authority.

4. Member States shall ensure that national competent authorities are provided with adequate financial and human resources to fulfil their tasks under this Regulation. In particular, national competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of artificial intelligence technologies, data and data computing,

fundamental rights, health and safety risks and knowledge of existing standards and legal requirements.

5. Member States shall report to the Commission on an annual basis on the status of the financial and human resources of the national competent authorities with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.

6. The Commission shall facilitate the exchange of experience between national competent authorities.

7. National competent authorities may provide guidance and advice on the implementation of this Regulation, including to small-scale providers. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union legislation, the competent national authorities under that Union legislation shall be consulted, as appropriate. Member States may also establish one central contact point for communication with operators.

8. When Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as the competent authority for their supervision.

TITLE VII

EU DATABASE FOR STAND-ALONE HIGH-RISK AI SYSTEMS

Article 60
EU database for stand-alone high-risk AI systems

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Article 51.

2. The data listed in Annex VIII shall be entered into the EU database by the providers. The Commission shall provide them with technical and administrative support.

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

4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.

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

TITLE VIII

POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE

CHAPTER 1

POST-MARKET MONITORING

Article 61
Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

CHAPTER 2

SHARING OF INFORMATION ON INCIDENTS AND MALFUNCTIONING

Article 62
Reporting of serious incidents and of malfunctioning

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred.

   Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.

CHAPTER 3

ENFORCEMENT

Article 63
Market surveillance and control of AI systems in the Union market

1. The national supervisory authority shall report to the Commission on a regular basis the outcomes of relevant market surveillance activities. The national supervisory authority 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 high-risk AI systems, related to products to which legal acts listed in Annex II, section A apply, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under those legal acts.

3. 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 for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.

4. For AI systems listed in point 1(a) in so far as the systems are used for law enforcement purposes, points 6 and 7 of Annex III, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those systems.

5. Where Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as their market surveillance authority.

Article 64
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. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

3. 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 referred to in Annex III 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.

4. Where the documentation referred to in paragraph 3 is insufficient to ascertain whether a breach of obligations under Union law intended to protect fundamental rights has occurred, the public authority or body referred to paragraph 3 may make a reasoned request to the market surveillance authority to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within reasonable time following the request.

Article 65

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 referred to in Article 64(3). The relevant operators shall cooperate as necessary with the market surveillance authorities and the other national public authorities or bodies referred to in Article 64(3).

   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.

   The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the measures referred to in the second subparagraph.

3. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the operator to take.

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. Where, within three months of receipt of the information referred to in paragraph 5, 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.

6. 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.

Article 66
Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 65, objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without delay enter into consultation with the relevant Member State and operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within 9 months from the notification referred to in Article 65and notify such decision to the Member State concerned.

2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant AI system is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.

Article 67
Compliant AI systems which present a risk

1. Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State finds that although an AI system is in compliance with this Regulation, it presents a risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, 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.

2. The provider or other relevant operators shall ensure that corrective action is taken in respect of all the AI systems concerned that they have made available on the market throughout the Union within the timeline prescribed by the market surveillance authority of the Member State referred to in paragraph 1.

Article 68
Formal non-compliance

1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned:

   (a) the conformity marking has been affixed in violation of Article 49;

   (b) the conformity marking has not been affixed;

   (c) the EU declaration of conformity has not been drawn up;

(d) the EU declaration of conformity has not been drawn up correctly;

(e) the identification number of the notified body, which is involved in the conformity assessment procedure, where applicable, has not been affixed;

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the high-risk AI system being made available on the market or ensure that it is recalled or withdrawn from the market.

TITLE IX

FINAL PROVISIONS

Article 75
AI systems already placed on the market or put into service

1. This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts.

2. This Regulation shall apply to the high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [*date of application of this Regulation*], only if, from that date, those systems are subject to significant changes in their design or intended purpose.

Article 76
Evaluation and review

1. The Commission shall assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation.

2. By [*three years after the date of application of this Regulation]* and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

3. The reports referred to in paragraph 2 shall devote specific attention to the following:

(a) the status of the financial and human resources of the national competent authorities in order to effectively perform the tasks assigned to them under this Regulation;

(b) the state of penalties, and notably administrative fines applied by Member States to infringements of the provisions of this Regulation.

4. Within [*three years after the date of application of this Regulation*] and every four years thereafter, the Commission shall evaluate the impact and effectiveness of codes of conduct to foster the application of the requirements set out in Title III, Chapter 2

and possibly other additional requirements for AI systems other than high-risk AI systems.

5. For the purpose of paragraphs 1 to 4 the Board, the Member States and national competent authorities shall provide the Commission with information on its request.

6. In carrying out the evaluations and reviews referred to in paragraphs 1 to 4 the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.

7. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology and in the light of the state of progress in the information society.

Article 85
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. This Regulation shall apply from [24 months following the entering into force of the Regulation].

3. By way of derogation from paragraph 2:

   (a) Title III, Chapter 4 and Title VI shall apply from [three months following the entry into force of this Regulation];

   (b) Article 71 shall apply from [twelve months following the entry into force of this Regulation].

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*